ITAT 教育部实用型信息技术人才培养系列教材

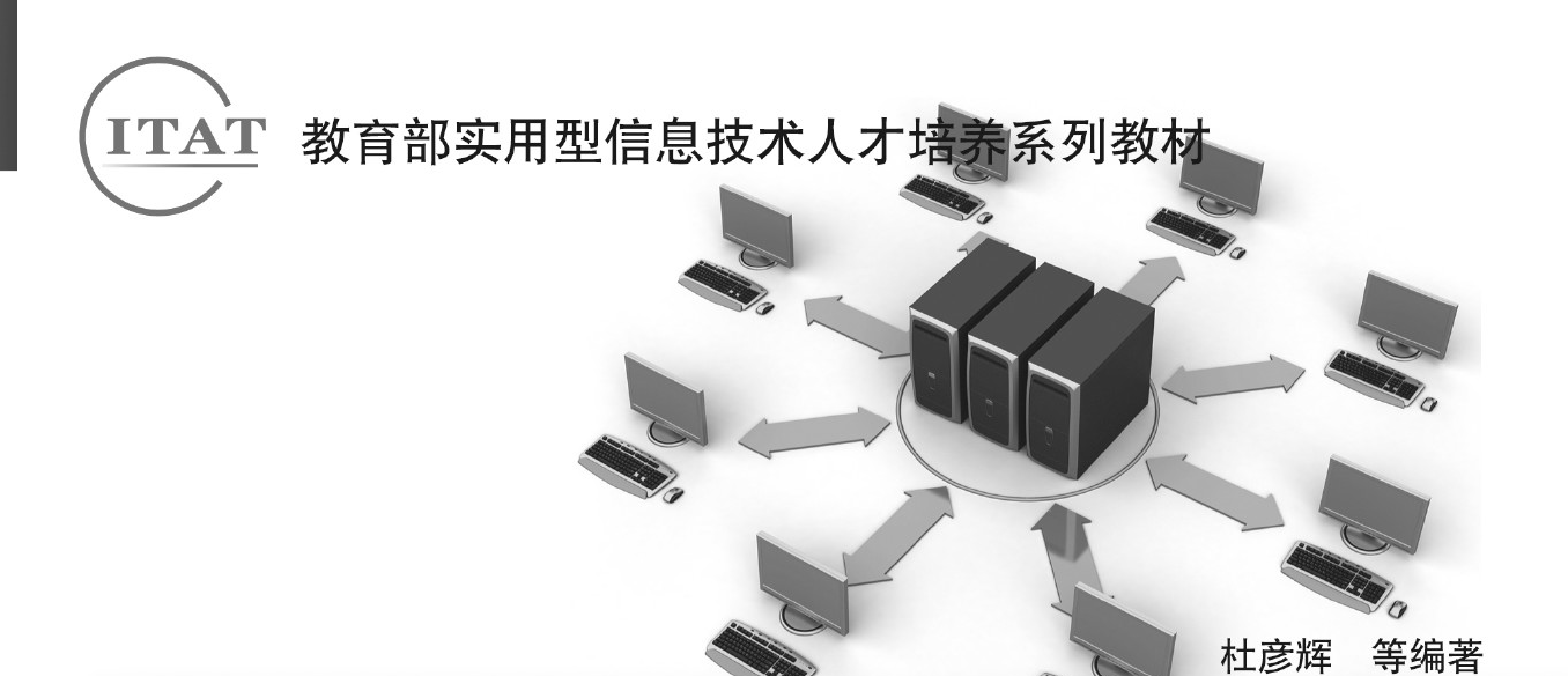


杜彦辉　等编著

信息安全技术教程

清华大学出版社

ITAT 教育部实用型信息技术人才培养系列教材



杜彦辉　等编著

信息安全技术教程

清华大学出版社

北　京

内 容 简 介

本书从信息安全领域的基础入手，系统、全面地介绍信息安全理论和实践知识，并尽可能地涵盖信息安全技术的主要内容，对发展起来的新技术做详细介绍。此外，还增加实践内容，介绍相关工具软件以及具体信息安全技术实施的具体方法。

本书共 19 章，主要内容包括信息安全基础知识、密码技术、认证技术、安全协议、安全事件处理、访问控制与权限设置、防火墙技术、入侵检测、系统安全扫描技术、病毒防范与过滤技术、信息安全风险评估技术、灾难备份与恢复技术、计算机与网络取证技术、操作系统安全、操作系统加固、安全审计原则与实践、应用开发安全技术、信息安全建设标准、构建企业安全实践等。

本书结构清晰、内容翔实，具有很强的可读性，适合作为高等院校信息安全专业本科生和相关专业的高年级本科生或研究生教材，也适合供相关科研人员和对信息安全相关技术感兴趣的读者阅读。

图书在版编目（CIP）数据

信息安全技术教程 / 杜彦辉等编著. —北京：清华大学出版社，2012
（IT&AT 教育部实用型信息技术人才培养系列教材）
ISBN 978-7-302-30524-8

Ⅰ. ①信…　Ⅱ. ①杜…　Ⅲ. ①信息安全-安全技术-教材　Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2012）第 258133 号

责任编辑：冯志强
封面设计：
责任校对：胡伟民
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**24.75　　**字　　数：**615 千字
版　　次：2013 年 1 月第 1 版　　**印　　次：**2013 年 1 月第 1 次印刷
印　　数：1~
定　　价：　　元

产品编号：037800-01

前 言

FOREWORD

本书针对信息安全领域的安全技术进行全面系统的介绍。随着信息网络技术的快速发展，信息安全技术也不断丰富和完善。本书尽可能涵盖信息安全技术的主要内容，对发展起来的新技术做介绍。同时增加实践内容，介绍相关工具软件以及信息安全技术实施的具体方法。

本书包含信息安全技术基础、网络安全技术、操作系统安全技术、信息安全产品技术、应用开发涉及的安全技术、信息安全建设、信息安全技术实践等内容。

第 1 章信息网络安全基本概念，主要讲述信息安全的基本概念，以及信息安全涉及的主要术语，如信息资产、系统漏洞和风险评估等。

第 2 章密码技术，密码学是信息安全技术基础，本章简单明了地介绍密码学原理、对称与非对称加密算法，以及数字签名、数字证书等主要应用技术。

第 3 章认证技术，本章在密码技术的基础上，介绍数字认证的过程、原理和应用。

第 4 章安全协议，基于 TCP/IP 安全协议，重点介绍基于 TCP/IP 的有关安全协议，包括应用层的安全协议等。

第 5 章安全事件处理，本章介绍网络攻击的过程、方法以及网络攻击的防范与响应技术。本章对主要的网络攻击手段进行分析，使读者对各种网络攻击有全面的了解。此外，对于网络安全发展的新技术，如无线网络安全、传感网络安全，也进行了介绍。

第 6 章访问控制与权限设置，介绍访问控制模型和方法、身份识别和认证技术的应用。

第 7 章防火墙技术，第 8 章入侵检测，第 9 章系统安全扫描技术，第 10 章病毒防范与过滤技术，这几章分别介绍主流的网络安全产品的原理，并对这些网络安全产品应用进行了说明。

第 11 章信息安全风险评估技术，介绍信息安全风险评估策略以及风险评估工具等内容。

第 12 章灾难备份与恢复技术，保持业务连续性是灾难备份技术的目标，本章讲述灾难防范技术、灾难响应技术、灾难恢复技术以及如何制订灾难备份与响应计划等内容。

第 13 章计算机与网络取证技术，本章重点介绍电子取证技术基础知识，包括电子证据内容、电子取证基本过程等，并对取证工具进行了介绍。

第 14 章操作系统安全，第 15 章操作系统加固，第 16 章安全审计原则与实践都是基于操作系统安全方面的安全技术，分别针对 Windows、UNIX/Linux 系列操作系统分析常见的安全问题，给出操作系统加固的具体方法，介绍操作系统中的安全审计策略和相关工具的使用。

第 17 章应用开发安全技术，介绍数据库应用以及软件开发过程中的安全技术。特别对 Web 技术以及电子商务过程中的安全技术进行了重点介绍。

第 18 章信息安全建设标准，第 19 章构建企业安全实践，这两章是信息安全实践内容，在介绍一般信息安全建设的通用原则的基础上，给出一般企业进行信息安全建设的

具体内容。

本书内容翔实、讲解透彻，具有如下特色。

（1）每章开始都列出本章的学习重点。每章的第一节介绍基本概念、背景知识。在此基础上对信息安全技术进行深入浅出的介绍。

（2）教材文字内容简洁、清晰，尽可能采用插图、表格、以及截图的方式进行说明。

（3）每章都包含有技术要点、小贴士以及一些提示读者注意的内容。

（4）每章都有习题，帮助读者复习本章的主要内容，掌握基本概念和基本原理。

（5）实践与思考，采用给出情景模拟，提出问题的方式，帮助读者进行扩展思路，更深入掌握信息安全的技术内涵。

（6）每章都给出扩展学习资源，提供开源工具软件下载以及扩展阅读列表。

本书由杜彦辉任主编，司响、李秋锐、杜锦、陈光宣参与编写。具体编写分工为：司响、李秋锐、杜锦、陈光宣共同编写第 1 章，司响负责编写第 2、3、6、7、9、10、14、15 和 19 章，李秋锐负责编写第 4、5、8、11、12、13、16 和 18 章。杜锦、陈光宣负责书稿的编写和审阅，全书由杜彦辉统稿和审阅。

由于时间仓促，不妥之处欢迎读者批评指正。

编　者

2012 年 5 月

目 录

CONTENTS

第 1 章　信息网络安全基本概念

本章学习重点：

- 介绍信息安全基本术语
- 了解网络环境下计算机安全复杂性
- 理解信息系统中面临的威胁种类
- 利用风险分析方法对信息资产进行分析，确定信息资产中面临的威胁/漏洞等潜在风险，并对信息进行风险管理

信息技术的迅速发展把人类推进到信息革命的历史潮流，信息革命成为人类第三次最伟大的生产力革命。数字化生存的方式、空间、时间不断开拓，信息成为当今社会中须臾不可离开的基本生活要素，比如银行账户信息、个人邮件数据等。如何保证计算机系统中存储数据的安全受到广泛关注。

1.1 信息安全基础

1. 计算机安全

计算机安全（Computer Security）是计算机与网络领域的信息安全（Information Security）的一个分支，其目标包括保护信息免受未经授权的访问、中断和修改，同时为系统的预期用户保持系统的可用性。计算机系统安全的定义是：为数据处理系统建立和采用的技术以及管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由于它的目的在于防止不需要的行为发生而非使得某些行为发生，其策略和方法常与其他大多数的计算机技术不同。

2. 网络安全

网络安全的研究对象是整个网络，研究领域比计算机系统安全更为广泛。网络安全的目标是要创造一个能够保证整个网络安全的环境，包括网络内的计算机资源、网络中传输及存储的数据和计算机用户。通过采用各种技术和管理措施使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等问题。网络安全涉及的领域主要包括密码学设计、各种网络协议的通信以及各种安全实践等。

3. 信息安全

信息安全作为一个更大的研究领域，对应信息化的发展，信息安全包含了信息环境、信息网络和通信基础设施、媒体、数据、信息内容、信息应用等多个方面的安全需要。信息安全是信息化社会的需要，是对应于信息不安全的状态，也是对应于人们努力的结

果。信息安全是为防止意外事故和恶意攻击而对信息基础设施、应用服务和信息内容的保密性、完整性、可用性、可控性和不可否认性进行的安全保护。

1.2 信息安全面临的挑战

1. 互联网体系结构的开放性

互联网是开放式体系结构，这种特性推动了互联网的迅速发展，加速了计算机产业和网际空间的发展，但同时，因为缺少整体的规划，当前很多协议制定是为了弥补之前的设计漏洞，蓝图的缺失带来了计算机网络基础设施和协议中的各种风险。

同时，网络基础设施和协议的设计者遵循着一条原则——尽可能创造用户友好性、透明性高的接口，使得网络能够为尽可能多的用户提供服务，但这样也带来了另外的问题：一方面用户容易忽视系统的安全状况，另一方面也引来了不法分子利用网络的漏洞来满足个人的目的。

2. 网络基础设施和通信协议的缺陷

伴随开放式的系统结构而产生的问题是网络通信协议中存在的漏洞。互联网是一个数据包网络，数据在传输的时候首先要被分为很多小的数据包，然后每一个数据包各自在网络中传输。在接收方，数据包又被重新组合构成原来的消息。为了能够正常工作，数据包网络需要在传输节点之间存在一个信任关系。

由于在传输过程中，数据包需要被拆分、传输和重组，所以必须保证每一个数据包以及中间传输单元的安全。然而，目前的网络协议并不能做到这一点。

网络中的服务器主要有 UDP 和 TCP 两个主要的通信协议，都使用端口号来识别高层的服务。客户端上的每个服务利用唯一的端口号向服务器请求服务，服务器利用端口号来识别客户所请求的服务。服务器的一个重要的安全规则就是当服务没有被使用的时候，要关闭其所对应的端口号，如果服务器不提供相应的服务，那么端口就一直不能打开。即使服务器提供相应的服务，也只有当服务被合法使用的时候端口号才能被打开。

客户端和服务器进行通信之前，要通过三次握手过程建立 TCP 连接。首先，客户端向服务器发送一个同步（SYN）数据包；然后，服务器响应一个 ACK 位和 SYN 位置位的数据包；最后，客户端响应一个 ACK 位置位的数据包。图 1-1 给出了三次握手的过程。三次握手过程存在着半打开（half-open）问题，由于服务器对之前发起握手的客户端存在信任关系，就会使端口一直处于打开状态以等待客户端的通信，而这个特性往往会被恶意攻击者利用。

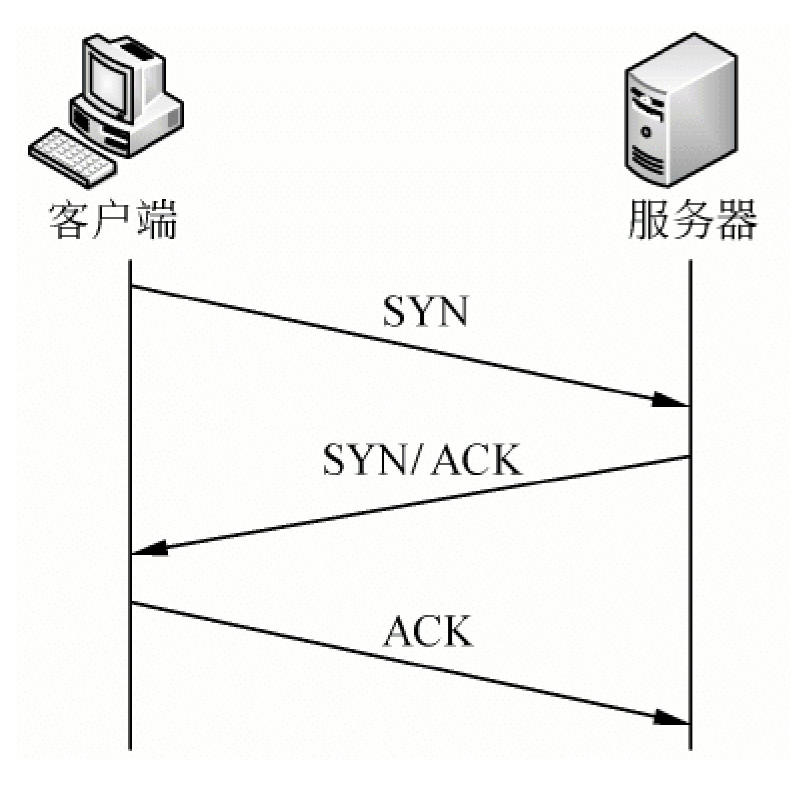


图 1-1　三次握手过程

3. 网络应用高速发展

造成安全问题的另一个原因是用户的数量激增。互联网自从 20 世纪 60 年代早期诞

生以来，得到了快速的发展，特别是最近10年时间，在用户使用数量和联网的电脑数量上有了爆炸式的增加。

随着计算机用户规模的扩大，当前许多国家的重要基础设施都连接在全球的网络中，同时由于互联网的易用性和低准入性的提高，很多恶意攻击者也进入网络，使得网络中存储的大量数据存在重大的安全隐患，对个人利益、企业利益和国家防御构成极大威胁。

4. 黑客

从普通用户角度来看，黑客是对计算机和网络通信构成威胁的最大因素，其通过使用病毒、蠕虫以及拒绝服务等攻击手段对计算机以及网络通信系统发动毁灭式的攻击，以获取个人利益。

黑客一词有着双重含义。现在，通常把试图突破信息系统安全、侵入信息系统的非授权用户称为黑客。然而，在计算机发展的早期，黑客通常是指那些精于使用计算机的人。

黑客的范围非常广泛，可以包含以下几类。

（1）窃取商业秘密的间谍。

（2）意在破坏对手网站的和平活动家。

（3）寻找军事秘密的间谍。

（4）热衷于恶作剧的青少年。

黑客们经常利用网络交流经验。在 Internet 上能很容易发现各种用于黑客交流技术手段以及最近实施攻击经验的网站。黑客可以在网站上找到用于攻击计算机和系统的知识。当然，这些网站对于安全管理者也有很大的帮助，用户同样可以得到这些知识，以避免受到同样的攻击。

5. 恶意软件

恶意软件（Malware，俗称“流氓软件”），也可以被称为广告软件（Adware）、间谍软件（Spyware）、恶意共享软件（Malicious Shareware）。与病毒或蠕虫不同，这些软件很多不是小团体或者个人秘密地编写和散播的，反而有很多知名企业和团体涉嫌此类软件。

恶意软件是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵犯用户合法权益的软件。恶意软件具有以下特点。

- **强制安装**　指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装软件的行为。
- **难以卸载**　指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍活动程序的行为。
- **浏览器劫持**　指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。
- **广告弹出**　指在未明确提示用户或未经用户许可的情况下，利用安装在用户计算机或其他终端上的软件弹出广告的行为。
- **恶意收集用户信息**　指未明确提示用户或未经用户许可，恶意收集用户信息的行为。
- **恶意卸载**　指未明确提示用户、未经用户许可，或误导、欺骗用户卸载非恶意

软件的行为。

❑ **恶意捆绑** 指在软件中捆绑已被认定为恶意软件的行为。

其他侵犯用户知情权、选择权的恶意行为。

6. 操作系统漏洞

软件错误是造成计算机系统严重安全威胁的重要因素之一，尤其是网络操作系统的错误。操作系统不但对于方便快捷地使用计算机系统起到重要的作用，而且在系统安全方面也起到了关键作用。攻击者会利用操作系统的漏洞取得操作系统中高级用户的权限，进行更改文件，安装和运行软件，格式化硬盘等操作。

每一款操作系统问世的时候本身都存在一些安全问题或技术缺陷。事实上，操作系统的安全漏洞是不可避免的。黑客常寻找操作系统的辨识信息来发现操作系统的漏洞，利用这些系统的漏洞实施攻击或破坏。

7. 内部安全

恶意的内部攻击是另外一种对系统安全构成重大威胁的因素。这是一种最为隐秘的威胁，同样也是最难被阻止的威胁，因为涉及合法用户的背叛。现在绝大多数的安全系统都会阻止恶意攻击者靠近系统，用户面临的更为困难的挑战是控制防护体系的内部人员进行破坏活动。

在组织内部需要特别注意安全专家和系统管理员。这些人拥有访问系统的极大权限，一旦有了不良企图，就会对组织造成严重影响。因此在设计安全控制时应该注意不要给某一个人赋予过多的权利。

8. 社会工程学

社会工程学（Social Engineering）是一种利用受害者心理弱点、本能反应、好奇心、信任、贪婪等心理缺陷进行诸如欺骗、伤害等危害手段取得自身利益的手法，近年来已成迅速上升甚至泛滥的趋势。社会工程学是通过搜集大量的信息，针对对方的实际情况进行心理战术的一种手法。通常以交谈、欺骗、假冒或口语等方式，从合法用户中套取用户系统的秘密。

实施社会工程学的手段有很多，可以通过网络、电话，甚至书信方式扮演拥有系统访问权的用户。

1.3 信息安全五性

1. 保密性

保密性服务用于保护系统数据和信息免受非授权的泄密攻击。当数据离开一个特定系统，例如网络中的服务器，就会暴露在不可信的环境中。所以数据的接收者就有理由怀疑在数据通信的过程中有可能会受到恶意攻击者的窃取。因此，保密性服务就是通过加密算法对数据进行加密，确保其处于不可信环境中也不会泄露。

在网络环境中，对数据保密性构成最大威胁的是嗅探者。嗅探者会在通信信道中安装嗅探器，检查所有流经该信道的数据流量。而加密算法是对付嗅探器的最好手段。加密通过一个加密算法和一个密钥对数据进行处理，数据处理前称为明文，处理后称为密文。加密算法分为对称和非对称两种，对称加密算法中加密方与解密方有相同的密钥，在算法过程中，加密与解密共用一个相同密钥；而非对称加密算法有两个密钥：一个可公开的公钥和一个需要妥善保管的密钥，通信过程中，发送方使用接收方发布的公钥进行加密，加密后只有接收方的密钥才可以进行解密。

2. 完整性

完整性服务用于保护数据免受非授权的修改，因为数据在传输过程中会处于很多不可信的环境，其中存在一些攻击者试图对数据进行恶意修改。Hash 算法是保护数据完整性的最好方法，Hash 算法对输入消息进行相应处理并输出一段代码，称为该信息的消息摘要。Hash 函数具有单向性，所以在发送方发送信息之前会附上一段消息摘要，用于保护其完整性。

3. 可用性

可用性服务用于保证合法用户对信息和资源的使用不会被不正当地拒绝。在不可信的网络环境中，有很多攻击者试图通过一些不合理的请求来阻碍系统正常工作，导致系统无法正常为合法用户提供服务。可用性的降低能够直接降低系统资源的价值，常见的攻击为拒绝服务攻击。

4. 可控性

可控性的关键为对网络中的资源进行标识，通过身份标识达到对用户进行认证的目的。一般系统会通过使用“用户所知”或“用户所有”来对用户进行标识，从而验证用户是否是其声称的身份。一般来说，认证的因素通常包括用户名、密码、视网膜、指纹、物理位置和身份卡等，其中视网膜和物理位置说明如下。

- **视网膜** 用户的眼睛对准一个电子设备，该电子设备可以记录用户的视网膜信息，根据该信息可以准确标识用户身份。
- **物理位置** 系统初始设置一个入口，只有规定位置的请求才可以进入。在网络环境中，可以检查被认证的客户端的 IP 地址来进行认证。而这种方法往往不是非常可靠的，所以常与其他的认证因素配合使用。

5. 不可否认性

不可否认服务用于追溯信息或服务的源头。在现实社会中，有些发送方可能拒绝承认该消息或信息是由其发出的，而在网络环境中，这种情况同样可能发生。为了制止这种情况的出现，可使用数字签名技术，通过数字签名使其信息具有不可替代性，而信息的不可替代性可以导致两种结果。

（1）在认证过程中，双方通信的数据可以不被恶意的第三方肆意更改。

（2）在认证过程中，信息具有高认证性，并且不会被发送方否认。

1.4 信息安全风险分析

1. 信息资产确定

信息资产大致分为物理资产、知识资产、时间资产和名誉资产 4 类。

- **物理资产** 具有物理形态的资产，例如：服务器，网络连接设备，工作站等。
- **知识资产** 其可以为任意信息的形式存在，例如：一些系统软件，数据库或者组织内部的电子邮件等。
- **时间资产** 对于组织与企业来说，时间也属于一种宝贵的财产。
- **名誉资产** 公众对于一个企业的看法与意见也可以直接影响其业绩，所以名誉也属于一种重要的资产，需要被保护。

2. 信息安全评估

对资产进行标识后，下一步就是对这些资产面临的威胁进行标识，首先有以下关键词便于理解这些风险。

- **安全漏洞** 安全漏洞即存在于系统之中，可以用于越过系统的安全防护。
- **安全威胁** 安全威胁是一系列可能被利用的漏洞。
- **安全风险** 当漏洞与安全威胁同时存在时就会存在安全风险。

三者的关系如图 1-2 所示。

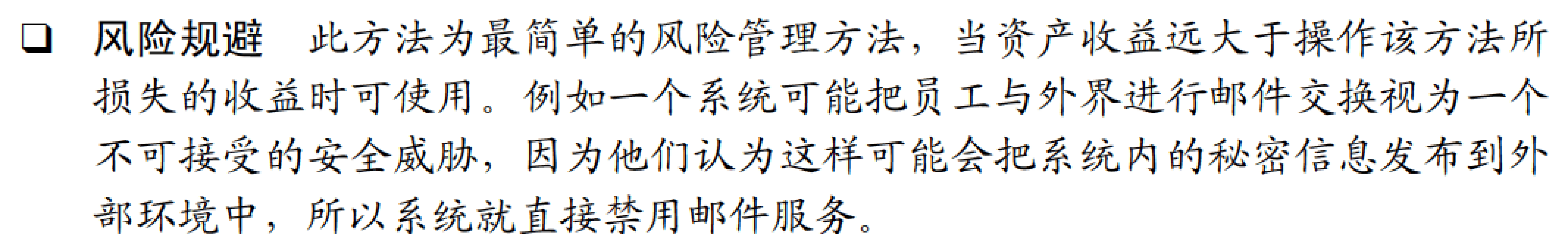


图 1-2 安全漏洞、安全威胁和安全风险三者关系

3. 风险管理

在确定了资产与资产面临的威胁后，应该对这些资产进行风险管理。具体来说，风险管理分为 4 个部分：风险规避、风险最小化、风险承担、风险转移。

- **风险规避** 此方法为最简单的风险管理方法，当资产收益远大于操作该方法所损失的收益时可使用。例如一个系统可能把员工与外界进行邮件交换视为一个不可接受的安全威胁，因为他们认为这样可能会把系统内的秘密信息发布到外部环境中，所以系统就直接禁用邮件服务。
- **风险最小化** 对于系统来说，风险影响最小化是最为常见的风险管理方法，该方法的具体做法是管理员进行一些预防措施来降低资产面临的风险，例如，对于黑客攻击 Web 服务器的威胁，管理员可以在黑客与服务器主机之间建立防火墙来降低攻击发生的概率。
- **风险承担** 管理者可能选择承担一些特定的风险，并将其造成的损失当作运营成本，这一方法称为风险承担。这种情况往往出现在危险发生的概率是极其低的（例如交通设备撞上数据中心）或者是不可避免的（例如硬盘工作中的磨损）情况下，当管理员选择了这一风险进行风险承担时，就会将其视为无风险。
- **风险转移** 作为风险转移，最为常见的例子就是保险，当一个人对自己身体健

康状态担忧时，为了对抗生病的风险，可以为自己投入保险，保险公司同意将此风险转移，当自己身体状况真的出问题时，保险公司可以提供相应的资金帮助其进行治疗，同样的道理可以用在系统维护上面。

在现实世界中，以上 4 种方法都不是独立使用的，一般来说，企业或组织都可以对 4 种方法进行综合使用。

习　　题

一、选择题

1. 由来自于系统外部或内部的攻击者冒充为网络的合法用户获得访问权限的攻击方法是下列哪一项？（　　）

A. 黑客攻击

B. 社会工程学攻击

C. 操作系统攻击

D. 恶意代码攻击

2. 在信息安全性中，用于提供追溯服务信息或服务源头的是哪一项？（　　）

A. 不可否认性

B. 认证性

C. 可用性

D. 完整性

二、问答题

1. 简述客户端和服务器进行通信时的三次握手过程。

2. 如何理解信息安全五性？

课后实践与思考

风险评估方案

了解和熟悉风险评估的内容，具体如下。

- **风险评估准备**　确定评估范围、组织评估小组、评估目标、评估工具和评估方法。
- **风险因素识别**　资产识别、威胁识别、脆弱点识别。
- **风险评估方法**　问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

一、资产评估

1．资产识别（表 1-1）

表 1-1　资产识别

<table>
<tr><td rowspan="2">硬件资产</td><td>应用系统</td><td>资产名称</td><td>资产编号</td><td>维护人</td><td>型号配置</td><td>购机年限</td><td>整体负荷</td><td>重要性程度</td></tr>
<tr><td>网络系统</td><td>资产名称</td><td>资产编号</td><td>维护人</td><td>型号配置</td><td>购机年限</td><td>整体负荷</td><td>重要性程度</td></tr>
<tr><td colspan="2">文档和数据</td><td>资产名称</td><td>责任人</td><td>备份形式</td><td>存储形式</td><td>重要性程度</td><td>备注</td><td></td></tr>
<tr><td colspan="2">人力资产识别</td><td>岗位</td><td>岗位描述</td><td>姓名</td><td>备注</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">业务应用</td><td>资产名称</td><td>设计容量</td><td>系统负荷</td><td>厂商服务能力</td><td>重要性程度</td><td></td><td></td></tr>
<tr><td colspan="2">物理环境</td><td>资产名称</td><td>适用范围描述</td><td>适用年限</td><td>整体负荷</td><td>重要性程度</td><td></td><td></td></tr>
</table>

2．资产赋值（表 1-2）

表 1-2　资产赋值

硬件资产	应用系统	资产名称	机密性	完整性	可用性	重要性程度	备注	
	网络系统	资产名称	机密性	完整性	可用性	重要性程度	备注	
文档和数据		资产名称	机密性	完整性	可用性	重要性程度	备注	
软件		资产名称	机密性	完整性	可用性	重要性程度	备注	
物理环境		资产名称	机密性	完整性	可用性	重要性程度	备注	

资产评估机密性、完整性、可用性的赋值通过调查问卷来实现，问卷题目举例如下。

机密性	是否能够容纳具有不同密钥长度的各种加密机制？ 是否保证 SOAP 消息级的机密性？ 加密签名数据时，其摘要值是否被加密？（如果没有加密，攻击者是否可以借此推测明文，使得加密数据被破坏？） 是否保证网络传输层的机密性？
完整性	是否为加密后的数据再采用签名以确保初始化矢量的完整性不被破坏？（加密算法中使用的初始化矢量虽然可以解决为给定密钥和数据创建相同密文的安全问题，但初始化矢量本身也可能被修改，使上述问题再次出现。） 是否采用的多种签名格式？
可用性	加密的工具对递归深度或请求使用资源数量是否做限制？ 选择采用合适的预防措施以免受任何潜在的拒绝服务的攻击。

3．重要性程度的赋值

应用头脑风暴法，即根据风险预测和风险识别的目的和要求，组成专家组，通过会议形式让大家畅所欲言，而后对各位专家的意见进行汇总、综合，以得出最后的结论。

资产评估值=Round{log 2 [$2^{\text{机密性}}+2^{\text{完整性}}+2^{\text{可用性}}$]}

机密性∈（0，4），完整性∈（0，4），可用性∈（0，4），资产评估值∈（0，4）

二、威胁评估

威胁评估和等级划分如图 1-3 所示。

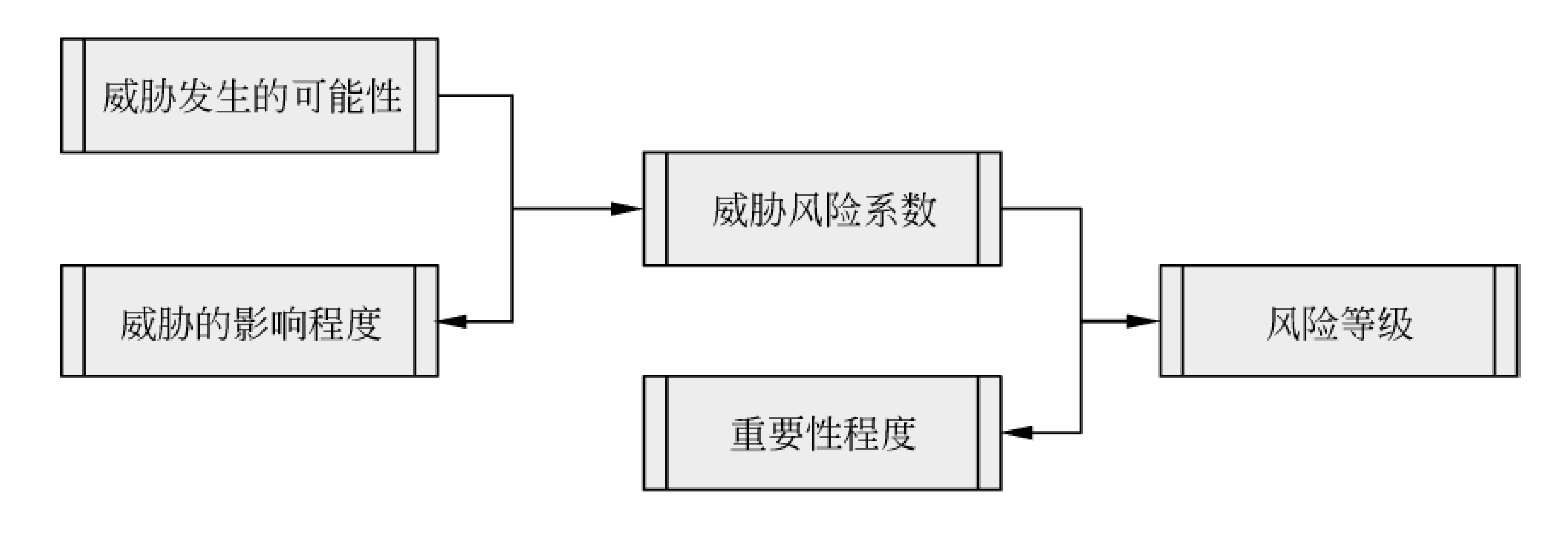


图 1-3　威胁评估和等级划分

风险等级划分见表 1-3。

表 1-3　风险等级划分

风险值≥900	极高	5	4
900＞风险值≥700	高	4	3
700＞风险值≥500	中	3	2
500＞风险值≥300	低	2	1
300＞风险值	极低	1	0

威胁的确定有以下两种方法。

（一）通过对应用系统、网络系统、文档和数据、软件、物理环境设计调查问卷，根据答案的汇总进行确定。

网络安全要素见表 1-4。

表 1-4　网络安全要素

网络层次	安全要素										
	身份鉴别	自主访问控制	标记	强制访问控制	数据流控制	安全审计	数据完整性	数据保密性	可信路径	抗抵赖	网络安全监控

网络安全功能基本要求说明如下。

（1）身份鉴别相关问题见表 1-5。

表 1-5　身份鉴别相关问题

用户识别	1．在 SSF 实施所要求的动作之前，是否对提出该动作要求的用户进行标识？ 2．所标识用户在信息系统生存周期内是否具有唯一性？ 3．对用户标识信息的管理、维护是否可被非授权地访问、修改或删除？
用户鉴别	1．在 SSF 实施所要求的动作之前，是否对提出该动作要求的用户进行鉴别？ 2．是否检测并防止使用伪造或复制的鉴别数据？ 3．能否提供一次性使用鉴别数据操作的鉴别机制？ 4．能否提供不同的鉴别机制？根据所描述的多种鉴别机制如何提供鉴别的规则？ 5．能否规定需要重新鉴别用户的事件？
用户-主体绑定	对一个已识别和鉴别的用户，是否通过用户-主体绑定将该用户与该主体相关联？

（2）自主访问控制相关问题见表 1-6。

表 1-6　自主访问控制相关问题

访问控制策略	1．是否按确定的自主访问控制安全策略实现主体与客体建操作的控制？ 2．是否有多个自主访问控制安全策略，且多个策略独立命名？
访问控制功能	1．能否在安全属性或命名的安全属性组的客体上执行访问控制 SFP？ 2．在基于安全属性的允许主体对客体访问的规则的基础上，能否允许主体对客体的访问？ 3．在基于安全属性的拒绝主体对客体访问的规则的基础上，能否拒绝主体对客体的访问？
访问控制范围	1．每个确定的自主访问控制，SSF 是否覆盖网络系统中所定义的主体、客体及其之间的操作？ 2．每个确定的自主访问控制，SSF 是否覆盖网络系统中所有的主体、客体及其之间的操作？
访问控制粒度	网络系统中自主访问控制粒度为粗粒度/中粒度/细粒度？

（3）标记相关问题见表 1-7。

表 1-7　标记相关问题

主体标记	是否为强制访问控制的主体指定敏感标记？
客体标记	是否为强制访问控制的客体指定敏感标记？
标记完整性	敏感标记能否准确表示特定主体或客体的访问控制属性？
有标记信息的输出	1．一客体信息输出到一个具有多级安全的 I/O 设备时，与客体有关的敏感标记也可输出吗？
	2．对于单级安全设备，授权用户能否可靠地实现指定的安全级的信息通信？

（4）强制访问控制相关问题见表 1-8。

表 1-8　强制访问控制相关问题

访问控制策略	是否为强制访问控制的主体指定敏感标记？
客体标记	是否为强制访问控制的客体指定敏感标记？
标记完整性	敏感标记能否准确表示特定主体或客体的访问控制属性？
有标记信息的输出	1．将一客体信息输出到一个具有多级安全的 I/O 设备时，与客体有关的敏感标记也可输出？
	2．对于单级安全设备，授权用户能否可靠地实现指定的安全级的信息通信？

（5）用户数据完整性相关问题见表 1-9。

表 1-9　用户数据完整性相关问题

存储数据的完整性	1．是否对基于用户属性的所有客体，对用户数据进行完整性检测？
	2．当检测到完整性错误时，能否采取必要的恢复、审计或报警措施？
传输数据的完整性	1．是否对被传输的用户数据进行检测？
	2．数据交换恢复若没有可恢复复件，能否向源可信 IT 系统提供反馈信息？
处理数据的完整性	对信息系统处理中的数据，能否通过“回退”进行完整性保护？

（6）用户数据保密性相关问题见表 1-10。

表 1-10　用户数据保密性相关问题

存储数据的保密性	是否对存储在 SSC 内的用户数据进行保密性保护？
传输数据的保密性	是否对在 SSC 内的用户数据进行保密性保护？
客体安全重用	1．将安全控制范围之内的某个子集的客体资源分配给某一用户或进程时，是否会泄露该客体中的原有信息？
	2．将安全控制范围之内的所有客体资源分配给某一用户或进程时，是否会泄露该客体中的原有信息？

具体调查问卷举例如下。

	调查问卷题目
认证	是否提供注册服务机制？
	只提供点到点的认证服务还是提供端到端的认证服务？
	是否更新现有的身份识别以符合最新 Web 服务安全规范？
授权	对访问资源提供大粒度的访问控制还是小粒度的访问控制？
	是否更新现有接入控制安全策略以满足服务安全规范？

续表

	调查问卷题目
	认证成功之后，　是否在运行时根据资源访问权限列表来检查服务请求者的访问级别？
审计性	管理员是否可以在生命周期的不同时刻追踪并找出服务请求？
	哪些技术提供了不可否认性的一个关键元素？
不可否认性	是否支持不可否认性？（不可否认性使得用户能够证明事务是在拥有合法证书的情况下进行的。）
	是否包含时间戳、序列号、有效期、消息相关等元素，并进行签名从而保证消息的唯一性？（当缓存这些信息时，可以检测出重放攻击。）

（二）通过工具进行扫描。

1．收费威胁扫描工具（内网威胁发现解决方案）。

- **核心技术**　已知病毒扫描、变种和加壳恶意程序扫描、恶意程序行为分析引擎、网络蠕虫病毒扫描、网页信誉服务。
- **能解决的问题**　恶意程序实时分析系统、恶意程序的深度分析、恶意程序的处置建议。
- **可得出的结论**　总体风险等级、感染源统计、威胁统计、潜在风险。

2．免费扫描工具。

- **Nmap**　网络安全诊断和扫描工具，进行端口扫描，是一款开放源代码的网络探测和安全审核的工具，它的设计目标是快速地扫描大型网络。
- **Nikto**　Web 服务器漏洞扫描工具，Nikto 是一款开源的（GPL）网页服务器扫描器，它可以对网页服务器进行全面的多种扫描。扫描项和插件可以自动更新。基于 Whisker/libwhisker 完成其底层功能。这是一款非常棒的工具，但其软件本身并不经常更新，最新和最危险的可能检测不到。
- **X-scan、ISS、Nessus**　漏洞扫描工具。

说明：

众多的自动化扫描工具当中，Nessus 是最值得称赞的。它基于 C/S 架构、插件结构的自动化扫描工具，可以免费使用，在线升级并随时获取国内外安全高手编写的最新漏洞的扫描插件。目前 Nessus 的插件个数已经超过 14000 个，而且这个数量正在急速上升，因为几乎全世界的安全人员都在使用这个工具，其中有很多黑客会向 Nessus 提供自己编写的插件。因此，使用 Nessus 进行扫描就像是全世界的顶尖安全人员都在用他们的技术在帮助人们检查网络中的缺陷。

可得出的结论：漏洞信息摘要、漏洞的详细描述、解决方案、风险系数。

3．免费风险评估系统

ASSET 是美国国家标准及时协会 NIST 发布的一个可用于安全风险自我评估的软件工具，采用典型的基于知识的分析方法，通过问卷形式自动完成信息技术系统的自我安全评估，由此了解系统的安全现状，并提出相对的对策。

ASSET 下载地址：http://icat.nist.gov。

其他常用风险评估系统见表 1-11。

表 1-11　其他常用风险评估系统

名称	@RISK	ASSET	BDSS	CORA	COBRA	CRAMM	RA/SYS	RiskWatch
体系结构	单机	单机	单机	单机	C/S	单机	单机	单机
所用方法	专家系统	基于知识	专家系统	过程式算法	专家系统	过程式算法	过程式算法	专家系统
定性/定量	定量	定性/定量结合	定性/定量结合	定量	定性/定量结合	定性/定量结合	定量	定性/定量结合
数据采集方式	调查文件	调查问卷	调查问卷	调查文件	调查文件	过程	过程	调查文件
输出结果	决策支持信息	提供控制目标和建议	安全防护措施列表	决策支持信息	结果报告、风险等级	结果报告、风险等级	风险等级、控制措施	风险分析综合报告

三、文档审计

（一）手动进行审计和分析

1．日志的检查和分析

通过对日志的查询和分析，快速对潜在的系统入侵做出记录和预测，对发生的安全问题进行及时总结。

（1）关键网络、安全和服务器日志进行备份。

（2）定期对关键网络、安全设备和服务器日志进行检查和分析，形成记录。

2．权限和口令管理

（1）对关键设备按最新安全访问原则设置访问控制权限，并及时清理冗余系统用户，正确分配用户权限。

（2）建立口令管理制度，定期修改操作系统、数据库及应用系统管理员口令，并有相关记录。

（3）登录口令修改频率不低于每月一次。

（4）登录口令长度的限制，并采用数字、字母、符号混排的方式。

（5）采取限制 IP 登录的管理措施。

3．实时监控记录

（1）对服务器、主干网络设备的性能进行 24 小时实时监控的记录进行检查。

（2）对服务器、主干网络设备的运行情况，对实时监控的记录进行检查。

（3）对网络流量、网站内容进行实时监控，对实时监控的记录进行检查。

（二）利用安全审计和文档安全工具

绿盟、天融信均有安全审计查阅工具。

可实现的功能如下。

（1）审计查阅：提供从审计记录中读取信息的能力。

（2）有限审计查阅：审计查阅工具应禁止具有读访问权限以外的用户读取审计信息。

（3）可选审计查阅：审计查阅工具应具有根据准则来选择要查阅的审计数据的功能，并根据某种逻辑关系的标准提供对审计数据进行搜索、分类、排序的能力。

四、模拟渗透测试

渗透测试工具通常包括黑客工具、脚步文件等，分为免费和收费两种。

（1）免费渗透测试工具：Dsniff。Dsniff 是一个优秀的网络审计和渗透测试工具，是一个包含多种测试工具的软件套件。

（2）收费渗透测试工具：天融信的渗透测试产品。

五、风险评估结果的确定

根据心理学家提出的“人区分信息等级的极限能力为 7±2”的研究理论，划分风险为 0～8 共 9 个等级，见表 1-12。

表 1-12　风险等级

等级	描述	等级	描述
0	风险度极低	5	风险度中上
1	风险度低	6	风险度高
2	风险度偏低	7	风险度较高
3	风险度中下	8	风险度极高
4	风险度中		

第 2 章　密 码 技 术

本章学习重点：

- 对称密码算法和非对称密码算法的原理及特点
- 在信息社会中密码技术的安全作用
- 数字签名技术
- 数字证书
- 信息隐藏技术
- 邮件加密软件 PGP 的原理及使用

2.1 密码学基础

2.1.1 密码学历史及密码系统组成

人们在远古时代就已经开始信息的保密活动，当时主要应用于战争，战场上信息的可靠传递往往能促使战争的胜利，对作战双方具有重要意义。步入信息社会之后，传统通信方式被淘汰，然而，现代化的数字通信模式并不能保证信息的安全，信息的完整性和保密性比以往任何时候都更加重要。密码技术在保护信息安全中发挥着越来越大的作用，实现防止信息泄露、保护个人隐私以及全球电子商务可信性的目的。

一个密码系统由以下 4 个基本部分组成。

- **明文**　要被发送的原文消息。
- **密码算法**　由加密和解密的数学算法组成。
- **密文**　明文经过加密算法加密之后得到的结果。
- **密钥**　在加密和解密过程中使用的一系列比特串。

一个密码算法包含一对可逆函数，一个用来加密，一个用来解密。加密过程使用加密算法和密钥把明文消息变为密文。一般情况下，密文通常是不可读的。因此，密文可以在不可信的信道中传输。

图 2-1 给出了一个密码系统基本的组成。其中 m 代表明文消息，c 代表密文消息，E 代表加密算法，D 代表解密算法，k 代表密钥。

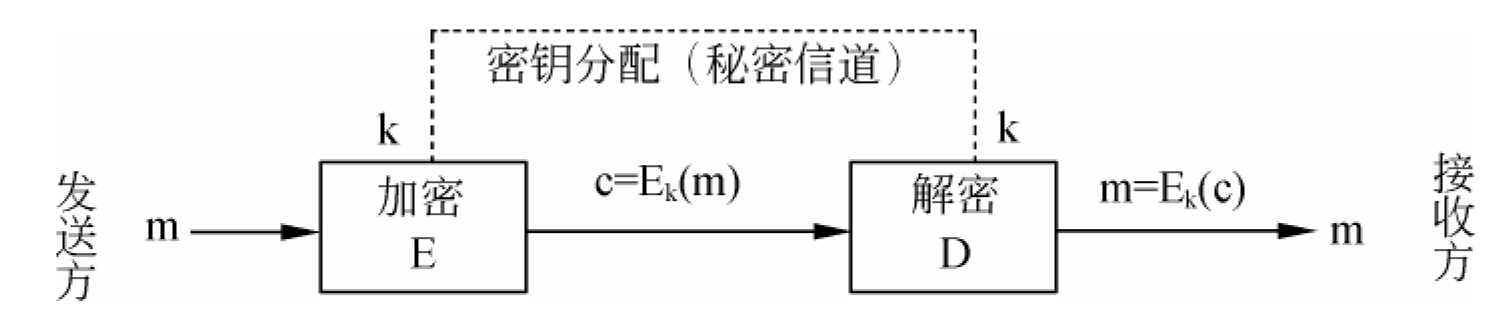


图 2-1　密码系统组成

2.1.2 密码的作用

通过应用密码技术可以实现信息的保密性、完整性、不可否认性和可控性。在一个密码系统中可以同时实现多个目标。例如，许多电子邮件的加密系统能同时实现保密性、完整性和不可否认性。

1. 保密性

消息的发送者使用密钥对消息进行加密。然后，消息以不可读的密文形式在介质中传输。在消息传输途中，拦截者不能读取消息的本意，从而达到了保密的目的。当消息到达目的地之后，接收者使用密钥对消息进行解密，恢复消息原文。

2. 完整性

密码可以保证被接收方收到的消息在传输过程中未经任何变动以保护其完整性。为了实现完整性，消息的发送者使用哈希函数为消息产生唯一的消息摘要，然后将消息摘要和消息一同传递。（消息摘要是由哈希函数产生的一串字符，每则消息的消息摘要是唯一的，并且任意两则消息的消息摘要都是不同的。）当这则消息到达目的地之后，接收者使用同样的哈希函数来计算它的消息摘要，并将其与所收到的消息摘要进行对比。如果这两个摘要是一致的，那么就可以认定消息在传输的过程中没有被修改。

正如上文所述，消息摘要只保障了消息免受非故意的更改（例如传输错误）。恶意第三方可以使用相同的哈希函数来产生一个新的消息摘要，进而欺骗接收方认为消息是真实的。基于这个原因，消息摘要通常被发送方加密之后再进行传输，这样就产生了数字签名。接收方通过验证数字签名能够保证消息没有被恶意的第三方修改。

3. 不可否认性

数字签名还可以向用户提供不可否认性。不可否认性保证了消息的发送者在发送消息之后不能否认曾经发送过消息。例如，一个顾客通过电子邮件发送了一个订单，那么，订单接收者就可以通过数字签名证明这个订单确实是顾客发送的而并非自己伪造的。

4. 可控性

用户或系统可以利用密码技术向其他的用户或系统来证明自己的身份，可以通过数字证书来完成。一个最普通的加密认证系统是 Kerberos 系统，在设计之初，此系统是使用在 UNIX 环境中的，而现在也适用于 Microsoft 环境。

2.1.3 密码算法

如前所述，一个密码算法由加密和解密算法组成，这是密码系统的核心，是实现加解密所必需的基本计算。根据加解密过程中是否使用了相同的密钥，可以将密码算法分成两类，对称密码算法和非对称密码算法。

理解一个密码算法基本功能最简单的方法是使用图示法。图 2-2 给出了密码算法的基本加密操作。明文在加密密钥的作用下，通过加密算法计算产生密文输出。

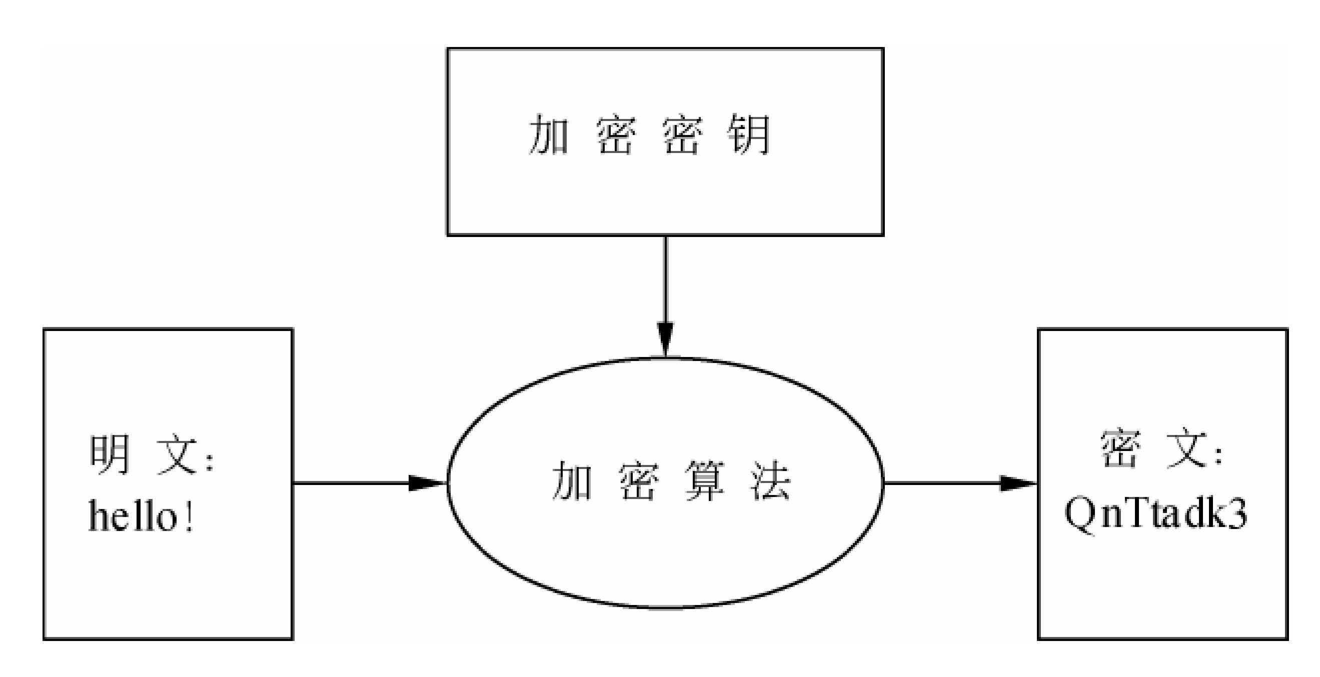


图 2-2　密码算法基本加密操作

反过来说，解密是相反的过程，如图 2-3 所示。密文输入后，在解密密钥的作用下，通过解密算法计算，产生明文输出。

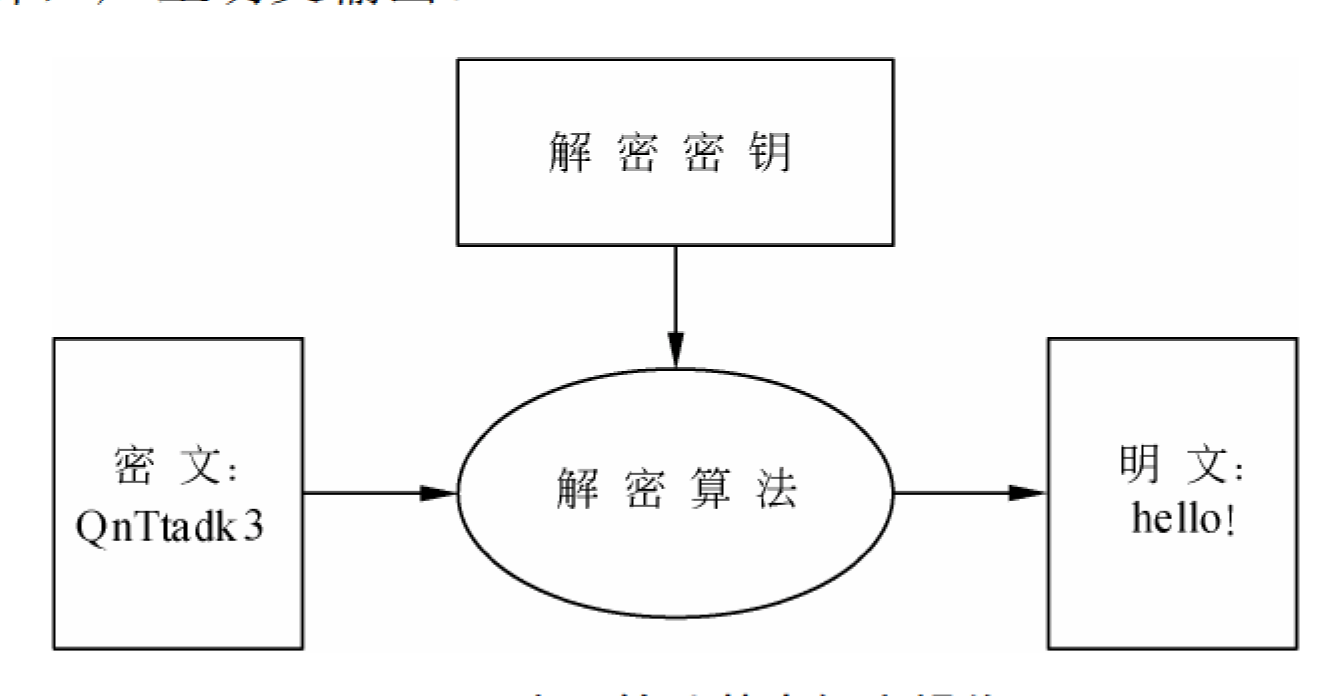


图 2-3　密码算法基本解密操作

2.2 对称密码算法

对称密码算法是指消息的发送者和接收者使用相同的密钥进行加密和解密的算法。这个密钥通常被称为共享密钥或秘密密钥。对称密码算法的安全性主要依赖于算法中所使用的密钥，密钥泄露就意味着任何人都可以对密文解密，所以密钥的保密对通信至关重要。

对称密码算法又被分为两类：流密码和分组密码。流密码是对明文消息按比特位进行加密（有些情况是按字节进行加密）。分组密码是对明文以分组为单位进行加密，每个明文分组通常是 64 比特或 128 比特。通用的分组密码包括 DES、AES、Blowfish、Twofish、Skipjack 和 RC2。最常见的流密码是 RC4。

2.2.1 DES 算法

DES 是最通用的一个对称密码算法，最早由美国政府开发。

1．算法描述

DES 是一种典型的分组密码，明文分组长度是 64 位，密钥的长度表面上是 64 位，

实际上有 8 位作为奇偶校验位，因此有效密钥长度是 56 位。

DES 使用密钥来自定义变换过程，只有持有加密所用的密钥的用户才能解密密文。密钥表面上是 64 位的，然而只有其中的 56 位被实际用于算法，其余 8 位被用于奇偶校验，并在算法中被丢弃。因此，DES 的有效密钥长度为 56 位，通常称 DES 的密钥长度为 56 位。

2．整体结构

算法的整体结构如图 2-4 所示：由 16 个相同的处理过程构成，并在首尾各有一次置换，称为 IP 与 IP^{-1}，IP^{-1} 为 IP 的反函数，即 IP “撤销” IP^{-1} 的操作，反之亦然。初始置换 IP 用于对明文中的各位进行换位，目的在于打乱明文中各位的顺序。IP 和 IP^{-1} 几乎没有密码学上的重要性，因此，为了简化硬件设计而被显式地包括在标准中。

在首次处理之前，数据分组被分成两个 32 位的块，并被分别处理；这种交叉的方式被称为 Feistel 结构。Feistel 结构保证了加密和解密过程足够相似——唯一的区别在于解密时子密钥是以反向顺序应用的，而剩余部分均相同。这样的设计大大简化了算法的实现，尤其是硬件实现，因为没有区分加密算法和解密算法的必要。

图中的 ⊕ 符号代表异或（XOR）操作。“F 函数”将数据半块与某个子密钥进行处理。然后，一个 F 函数的输出与另一个半块异或之后，再与原本的半块交换顺序，进入下一个循环的处理。在最后一个处理完成时，两个半块不必交换顺序，这是 Feistel 结构的一个特点，以保证加解密的过程相似。

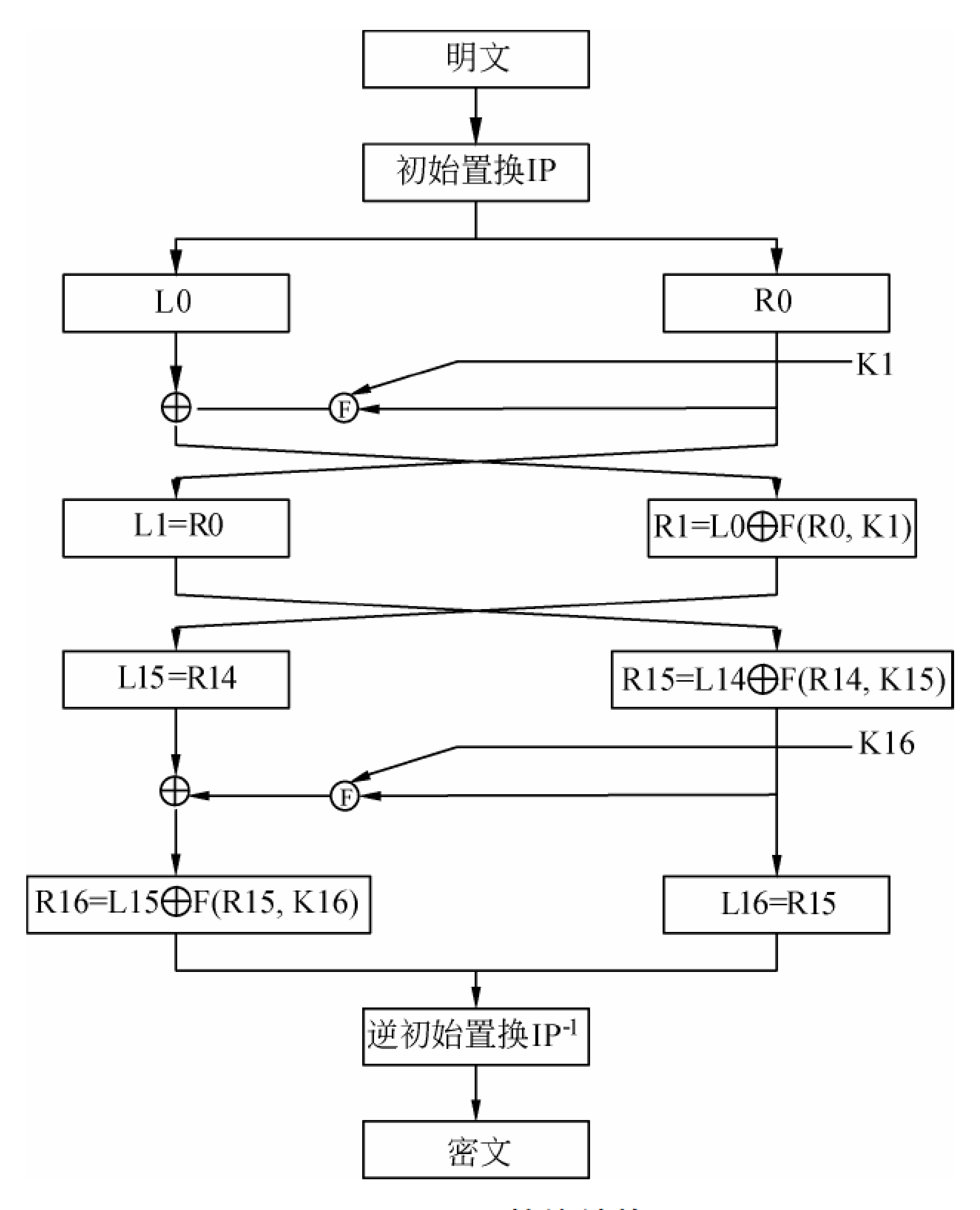


图 2-4　DES 整体结构图

3. F 函数

图 2-5 显示了 F 函数的数据处理过程，每次对半块（32 位）数据进行操作，并包括以下 4 个步骤。

（1）扩张。用扩张置换（图中的 E）将 32 位的半块扩展到 48 位。

（2）与密钥混合。用异或操作将扩张的结果和一个子密钥进行混合。16 个 48 位的子密钥——每个用于一个循环的 F 变换。

（3）S 盒。在与子密钥混合之后，分组被分成 8 个 6 位的块，然后使用“S 盒”，或称“置换盒”进行处理。每一个 S 盒都使用以查找表方式提供的非线性的变换，将 6 个输入位变成 4 个输出位。S 盒提供了 DES 的核心安全性——如果没有 S 盒，密码会是线性的，很容易破解。

（4）置换。最后，S 盒的 32 个输出位利用固定的置换，“P 置换”进行重组。

S 盒、P 置换和 E 扩张实现了密码的“混淆和扩散”。

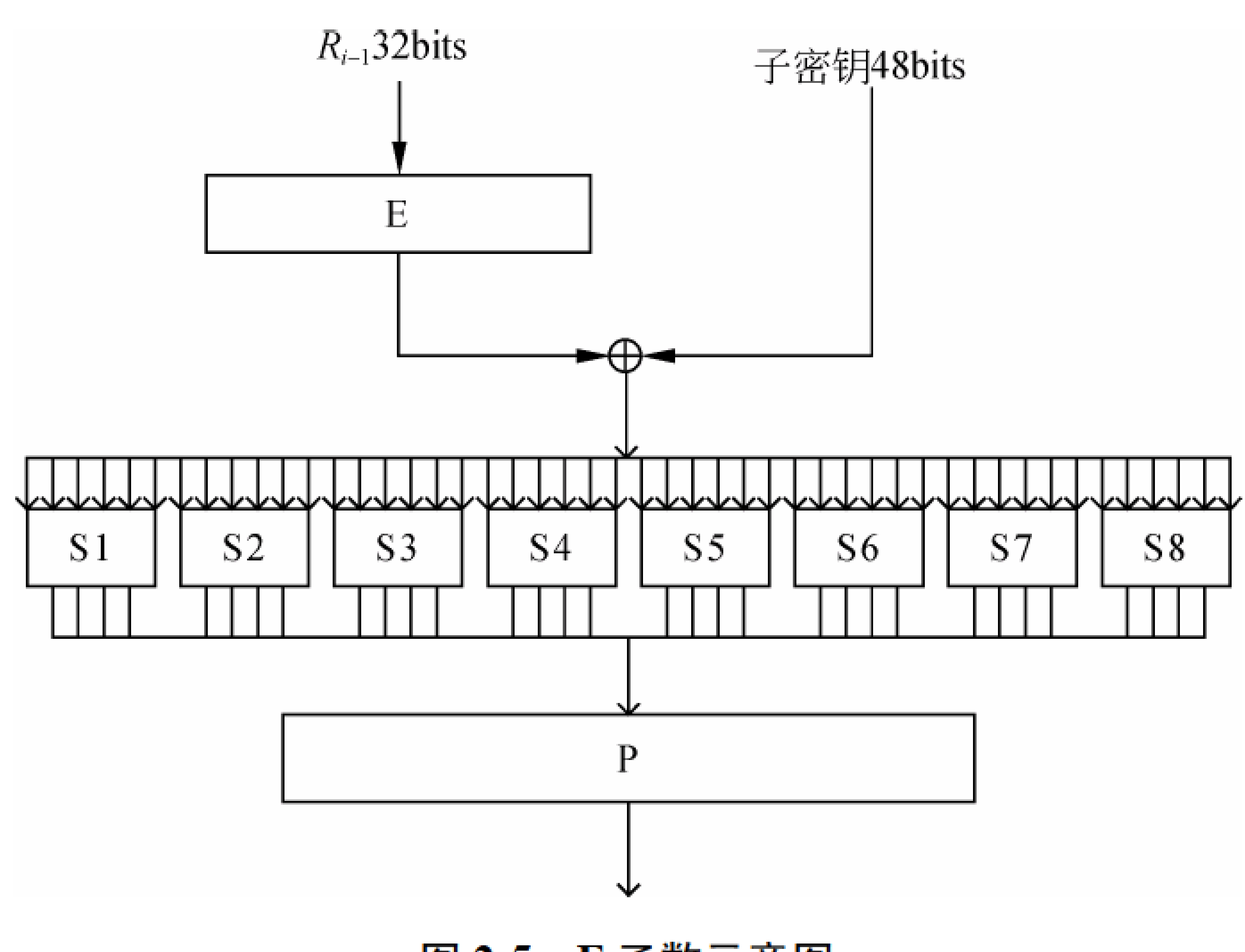


图 2-5　F 函数示意图

4. 密钥调度

图 2-6 显示了加密过程中的密钥调度——产生子密钥的算法。首先，使用选择置换 1（PC1）从 64 位输入密钥中选出 56 位的密钥，剩下的 8 位直接丢弃，或作为奇偶校验位。然后，56 位分成两个 28 位的半密钥，每个半密钥都被分别处理。在接下来的循环中，两个半密钥都被左移 1 或 2 位（由循环数决定），然后通过选择置换 2（PC2）产生 48 位的子密钥，每个半密钥 24 位。移位表明每个子密钥中使用了密钥中不同的位，每个位大致在 16 个子密钥中出现 14 次。

解密过程中，除了子密钥输出的顺序相反外，密钥调度的过程与加密完全相同。

DES 是一种极其灵活的密码算法，有多种运行模式。然而，DES 也存在着一个局限性，在现有的计算机水平上，56 比特的密钥长度不能提供足够的安全性能。为了克服这一局限性，密码学家研制开发了 3DES，即对一则消息进行 3 次 DES 的迭代加密，以增强安全特性。

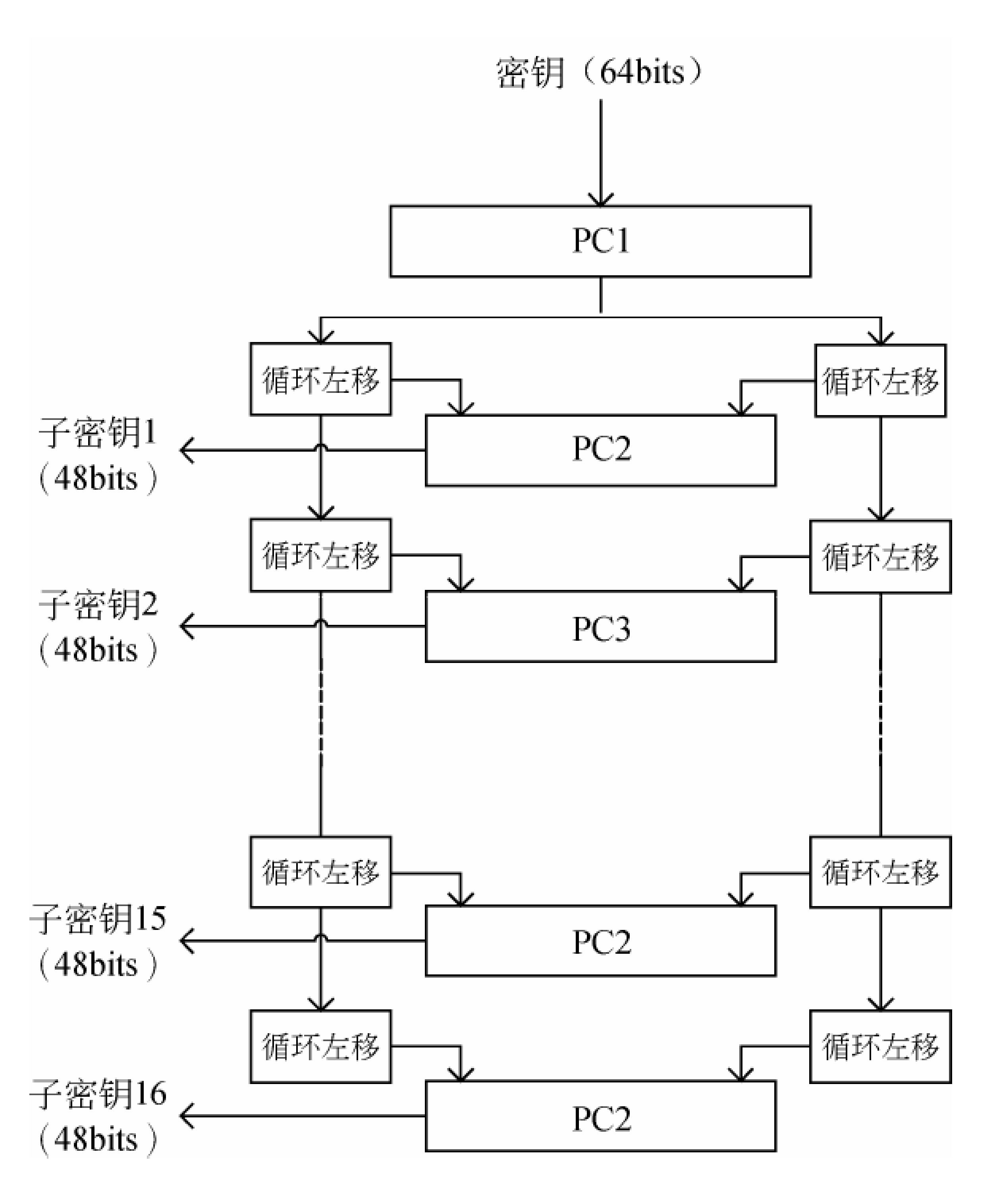


图 2-6　DES 算法中子密钥产生过程

2.2.2　对称密码算法存在的问题

对称密码算法运算量小，加密速度快，加密效率高，但加密前双方必须共享密钥这一性质也造成对称密码算法存在一定的问题。

（1）用户使用对称加密算法时，需要共享密钥，使得用户所拥有的钥匙数量成几何级数增长，密钥管理成为用户的负担。

（2）用户在通信之前，需要建立连接来产生和获取密钥。这对拥有庞大用户数量的网络的通信空间提出了很高的要求。

（3）密钥不能被及时更换以保证信息的保密性。

（4）消息的接收者不能检查消息在接收之前是否经过更改，数据的完整性得不到保证。

（5）无法保证接收到的消息来自于声明的发送者，因此，发送者能够对发送行为进行否认，不可否认性得不到保证。

2.3　非对称密码算法

非对称密码算法和对称密码算法最大的不同在于通信双方使用不同的密钥。事实上，每一个用户都拥有自己的一对密钥即一个公钥和一个私钥。公钥和私钥具有数学上的相关性，由其中一个密钥加密的消息只能由来自于同一密钥对的另一个密钥进行解密。另外，由公钥计算私钥在数学上是不可行的。通常，公钥用来加密，可以公开。私钥用来

解密，由用户自己保留。当某个用户想要和对方通信时，就使用对方的公钥对明文消息进行加密，然后把得到的密文消息传递给对方。对方收到密文之后，用自己的私钥解密，即可恢复出明文消息。因此，非对称密码算法通常又被称为公开密钥密码算法。

除了用于加密，当用户使用自己的私钥对消息进行加密，而使用公钥解密时，非对称密码算法还可以实现签名的功能，保证了数据的完整性。

2.3.1 RSA 算法

RSA 是最著名的公开密钥密码算法，由麻省理工学院的 3 名计算机安全专家（Rivest，Shamir，Adelman，如图 2-7 所示）于 20 世纪 70 年代设计完成。RSA 是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的所有密码攻击，已被 ISO 推荐为公钥数据加密标准。此算法基于大素数因式分解的困难性来产生公钥/私钥对。当用户想要加密或解密消息时，只要对明文或密文使用适当的密钥进行模运算，就可以得到相应的密文或明文输出。

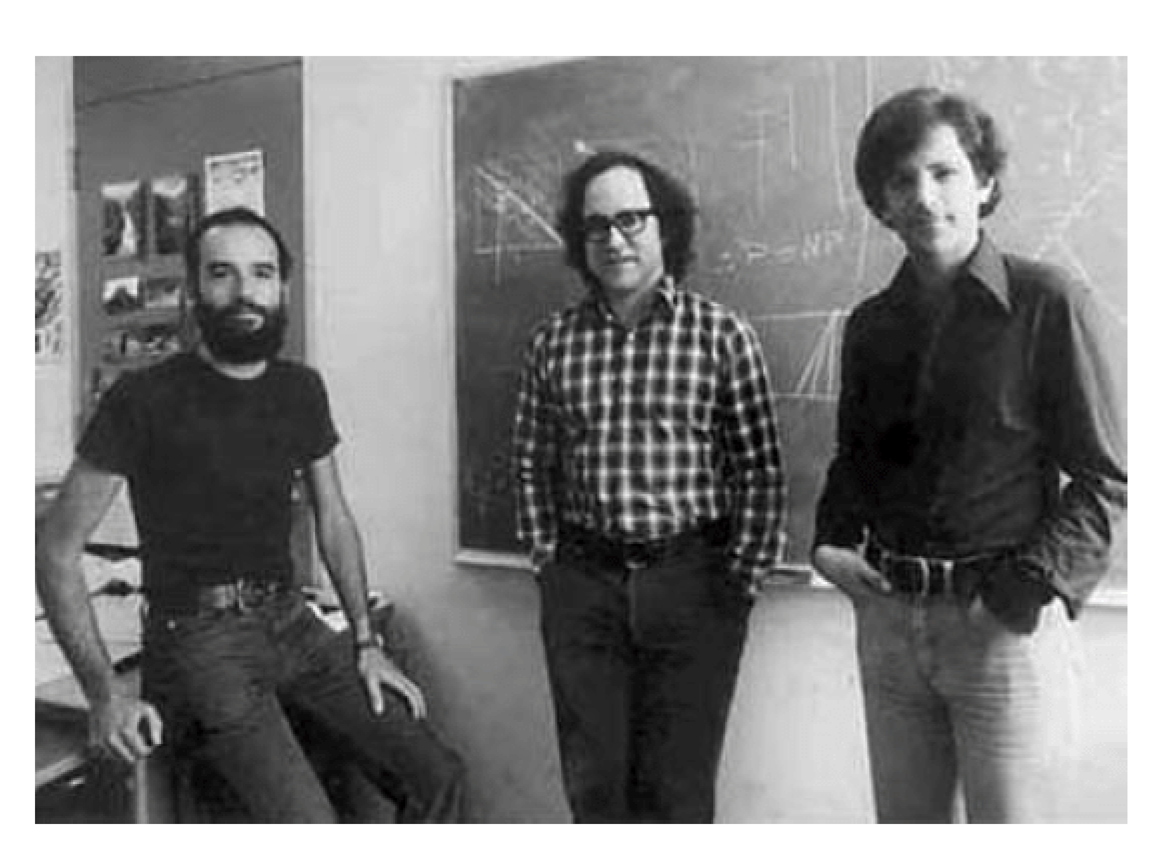


图 2-7　RSA 算法发明者（Ron Rivest、Adi Shamirh 和 Len Adleman）

RSA 密码体制如下。

1．公钥和私钥的产生

随机选择两个大素数 p 和 q，p 不等于 q，p 和 q 保密。

计算 n=pq，n 公开。

计算欧拉函数 $\phi(n)=(p-1)(q-1)$，$\phi(n)$ 保密。

随机选择整数 e，$1<e<\phi(n)$ 且 $\gcd(e,\ \phi(n))=1$，e 公开。

计算 d 满足：$de \equiv 1 \pmod{\phi(n)}$，d 保密。

(n，e)是公钥，(n，d)是私钥。

2．加密与解密过程

加密变换：对于明文 $m \in Z_n$，密文为

$c \equiv m^e \bmod n$

解密变换：对于密文 $c \in Z_n$，明文为

$$m \equiv c^d \bmod n$$

RSA 算法的加密解密过程如图 2-8 所示。

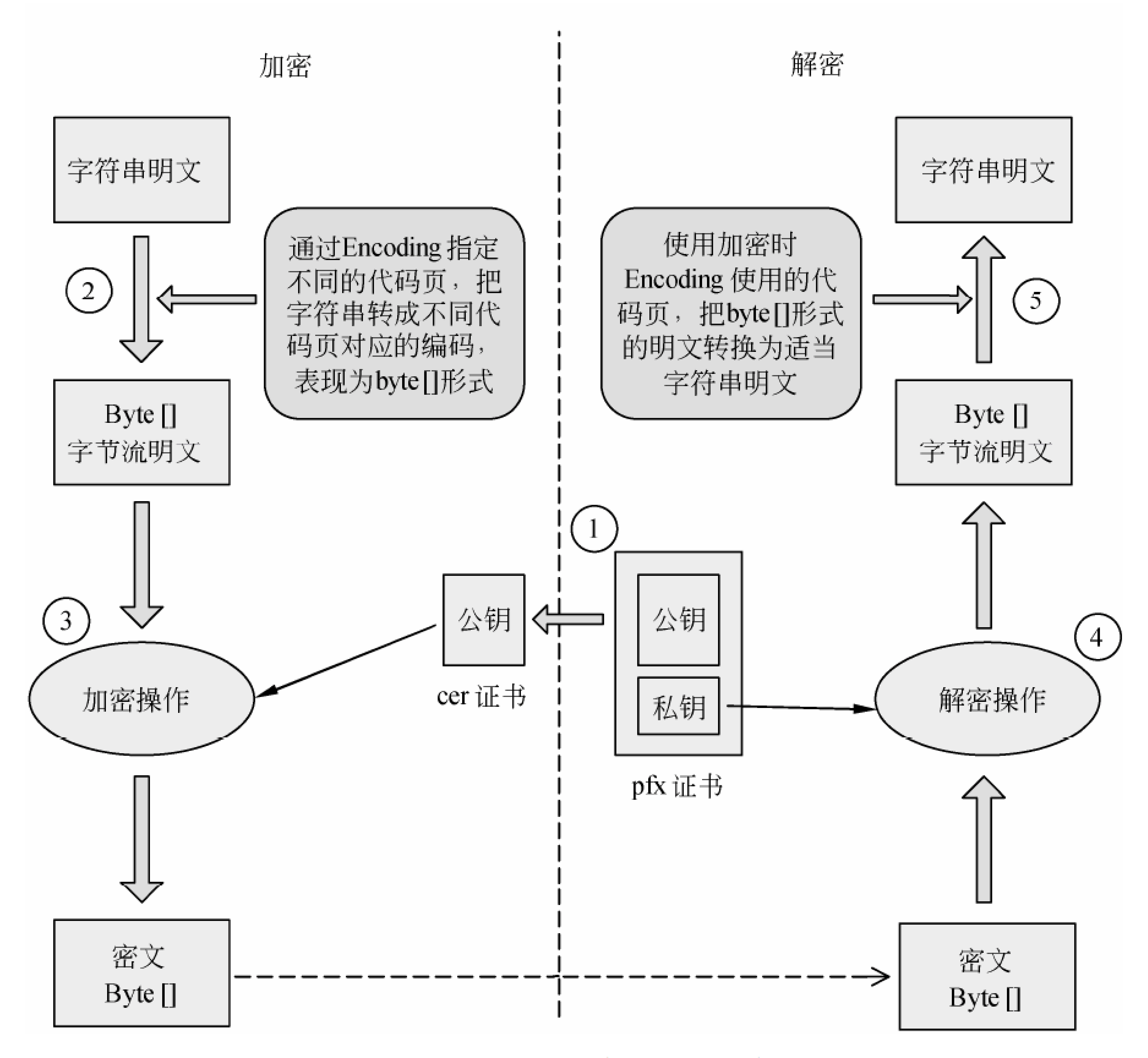


图 2-8　RSA 加密解密过程图解

3. RSA 应用举例

Alice 想要使用 RSA 算法与 Bob 通信。首先，Alice 计算公钥/私钥对。选 p=11，q=23，则 n=pq=253，$\phi(n)$=(p−1)(q−1)=220。选加密密钥 e=3，由 3×147≡1(mod 220)，得解密密钥 d=147。至此，Alice 的公钥对是(253，3)，私钥对是(253，147)。Alice 将公钥(253，3)传递给 Bob，自己保留私钥(253，147)。

设 Bob 向 Alice 传递的消息是 “A”，Bob 首先将消息转换成 ACSII 码形式（当然也可以选择其他方式），得 m=65。Bob 利用公钥(253，3)计算 $65^3 \equiv 120 \bmod 253$，得到密文 c=120。然后，Bob 将 c=120 通过信道传递给 Alice。

Alice 收到密文消息 c=120 之后，计算 $120^{147} \equiv 65 \bmod 253$，得到明文消息 m=65，则 Alice 知道 Bob 发送给自己的消息是 “A”。

2.3.2　非对称密码算法存在的问题

尽管非对称密码算法已经解决了对称算法的密钥交换和消息否认问题，但仍存在一

定问题。非对称密码算法最大的问题就是速度问题。因为在计算密钥时，需要对大整数进行幂运算。例如，像 RSA 这样速度最快的非对称密码算法比任何一种对称密码算法都要慢很多。因此，在对长消息进行加密时，非对称密码算法的速度就很难得到令人满意的结果。

另外，非对称密码算法还可能遭受中间人攻击。中间人攻击是一种常见的攻击方式，攻击者从通信信道中截获数据包并对其进行修改，然后再插回信道中，从而将自己伪装成合法的通信用户。

2.4 数字签名技术

数字签名可以增加密码系统的完整性和不可否认性。只有使用非对称密码系统时，数字签名才可能实现。

2.4.1 数字签名生成

要产生数字签名，首先要使用一个哈希函数来产生明文消息的消息摘要（MAC 值）。哈希函数是一种单向函数，并且能保证消息和消息摘要之间一对一的映射，也就是说，没有任何两个不同的消息能够产生相同的哈希值。

在 FIPS180-2 中，由美国国家标准技术研究所（NIST）发布了 4 个政府认可的哈希函数。每个都是安全哈希算法（SHA）的变种。

- **SHA-1** 对任何输入长度小于 2^{64} 比特的消息产生一个 160 比特的摘要。
- **SHA-256** 对任何输入长度小于 2^{64} 比特的消息产生一个 256 比特的摘要。
- **SHA-384** 对任何输入长度小于 2^{128} 比特的消息产生一个 384 比特的摘要。
- **SHA-512** 对任何输入长度小于 2^{128} 比特的消息产生一个 512 比特的摘要。

这些算法最终取代了 SHA 成为官方批准的美国政府标准。

另一种常见的哈希算法是由 Ronald Rivest 设计的消息摘要（MD）算法，有 3 种常见的 MD 算法。

- **MD2** 对任意长度的消息产生一个 128 比特的消息摘要，适用于 8 比特的处理器。
- **MD4** 对任意长度的消息产生一个 128 比特的消息摘要。但由于 MD4 算法存在引起冲突的漏洞，应该避免使用。
- **MD5** 对任意长度的消息产生一个 128 比特的消息摘要，适用于 32 位的处理器。MD5 检验互联网下载的文件的完整性，防止偶然的和蓄意的篡改。

消息摘要产生后，用户需使用私钥对其进行加密从而产生数字签名。之后，发送方使用和接收方共享的密钥将消息和数字签名加密后一同发送给接收方，从而实现不可否认性和完整性的保护。

2.4.2 数字签名认证

密码系统收到经过数字签名的消息后，可以通过以下的步骤对这个签名进行认证。

首先解密消息，提取出明文消息和数字签名。然后使用和发送方相同的哈希函数对明文消息进行计算，得到明文消息的消息摘要。同时，使用发送方的公钥解密数字签名。最后将发送方计算出的明文消息的消息摘要和由发送方解密出来的消息摘要进行比较。如果两个摘要是一样的，则能够认定消息在传递过程中未受到第三方的更改，通信的完整性得到了保护。同时，实现了消息的不可否认性，证明消息确实来自于发送者（得到发送者私钥的某些人）。数字签名认证过程如图 2-9 所示。

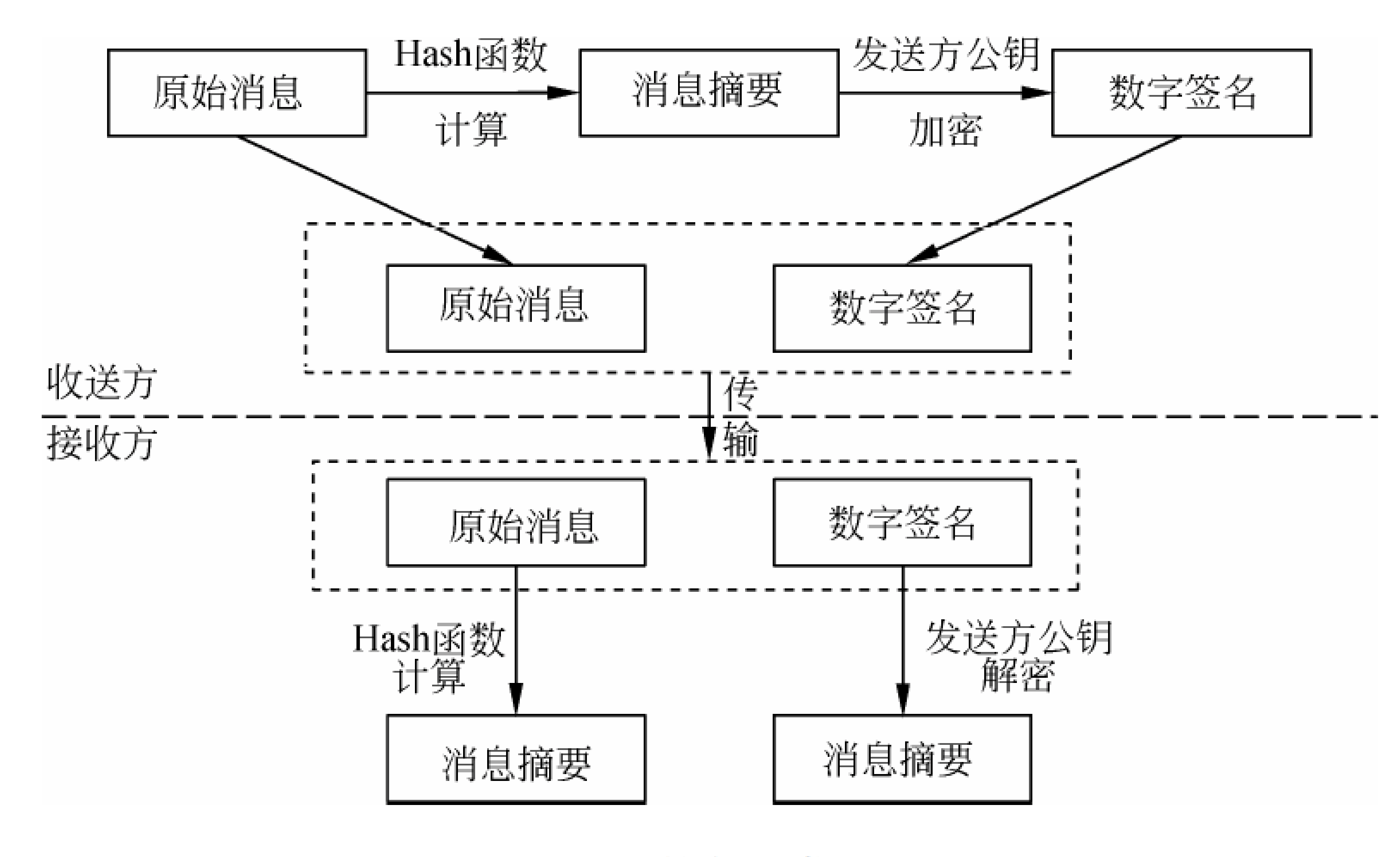


图 2-9　数字签名生成验证过程

如果两个摘要不一样，则可能是发生了一系列意外。这些情况包括以下几种。

（1）发送方和接收方之间发生传输错误。

（2）消息传输过程中，被第三方更改。

（3）消息是伪造的。

（4）通信的一方不正确地使用了密码软件。

2.5 数字证书

数字证书是由权威公正的第三方机构（CA 中心）签发的证书，它能提供在因特网上进行身份验证的一种权威性电子文档，人们可以在互联网交往中用它来证明自己的身份和识别对方的身份。在数字证书认证的过程中，证书认证中心（CA）作为权威的、公正的、可信赖的第三方机构，其作用极其关键。

以数字证书为核心的加密技术可以对因特网上传输的信息进行加密和解密、数字签名和签名验证，以确保网上传递信息的机密性、完整性。因此，数字证书广泛应用于收发安全电子邮件、网上银行、网上办公、网上交易、访问安全站点等安全电子事务处理和安全电子交易活动。即使发送的信息在网上传递过程中被他人截获，甚至丢失了个人的账户、密码等信息，仍可以保证账户、资金安全。

最简单的数字证书包含一个公开密钥、名称以及证书授权中心的数字签名。通常情况下，数字证书中还包括密钥的有效时间、发证机关(证书授权中心)的名称、证书的序列号等信息，证书的格式遵循 ITUT X.509 国际标准。一个标准的 X.509 数字证书包含以

下基本内容。

（1）证书的版本信息。

（2）证书的序列号，每个证书都有一个唯一的证书序列号。

（3）证书所使用的签名算法。

（4）证书的发行机构名称，命名规则一般采用 X.500 格式。

（5）证书的有效期，现在通用的证书一般采用 UTC 时间格式，它的计时范围为 1950—2049。

（6）证书所有人的名称，命名规则一般采用 X.500 格式。

（7）证书所有人的公开密钥。

（8）证书发行者对证书的签名。

2.5.1 数字证书的工作原理

数字证书以加密解密为核心，它采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把私有密钥（私钥，仅用户本人所知），然后用它进行解密和签名；同时，用户设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。当发送方准备发送一份保密文件时，先使用接收方的公钥对数据文件进行加密，而接收方则使用自己的私钥对接收到的加密文件进行解密，这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。在公开密钥密码体制中，比较常用的是 RSA 体制。

公开密钥体制解决了密钥发布的管理问题：网上商家可以保留其私钥，而公开发布其公钥；购物者可以用公开发布的公钥对发送的信息进行加密，安全地传送给网上商家，然后由商家用自己的私钥对其进行解密。

用户也可以运用自己的私钥对信息进行处理，由于密钥仅为用户本人所有，所以就产生了其他人无法生成的独一的文件，也就所谓的数字签名。采用数字签名，能够保证以下两点。

（1）保证信息是由签名者签名发送的，签名者不能予以否认或难以否认。

（2）保证信息自签发后到收到为止未曾作过任何修改，签发的文件是真实文件。

数字证书里存有很多数字和英文，当使用数字证书进行身份认证时，它将随机生成 128 位的身份码（每份数字证书都能生成相应的身份码，且每次都不可能相同的），相当于生成一个复杂的密码，从而保证数据传输的保密性。 其工作原理如图 2-10 所示。

数字证书一个最主要好处是在认证用户身份时，用户的敏感个人资料并不会传输至索取资料者的计算机系统上。通常，当索取资料者取得用户的数字证书资料后，会即时递交至数字核证机关的系统中进行验证。当用户身份经确认后，核证机关会将已经确认的信息转交至索取资料者，在此期间，除用户同意并主动给出的个人资料以外，其他资料均不会自动传递至索取资料者。透过这种资料交换模式，用户既可证实自己的身份，亦不用过度披露个人资料，对保障计算机服务存取双方皆有好处。

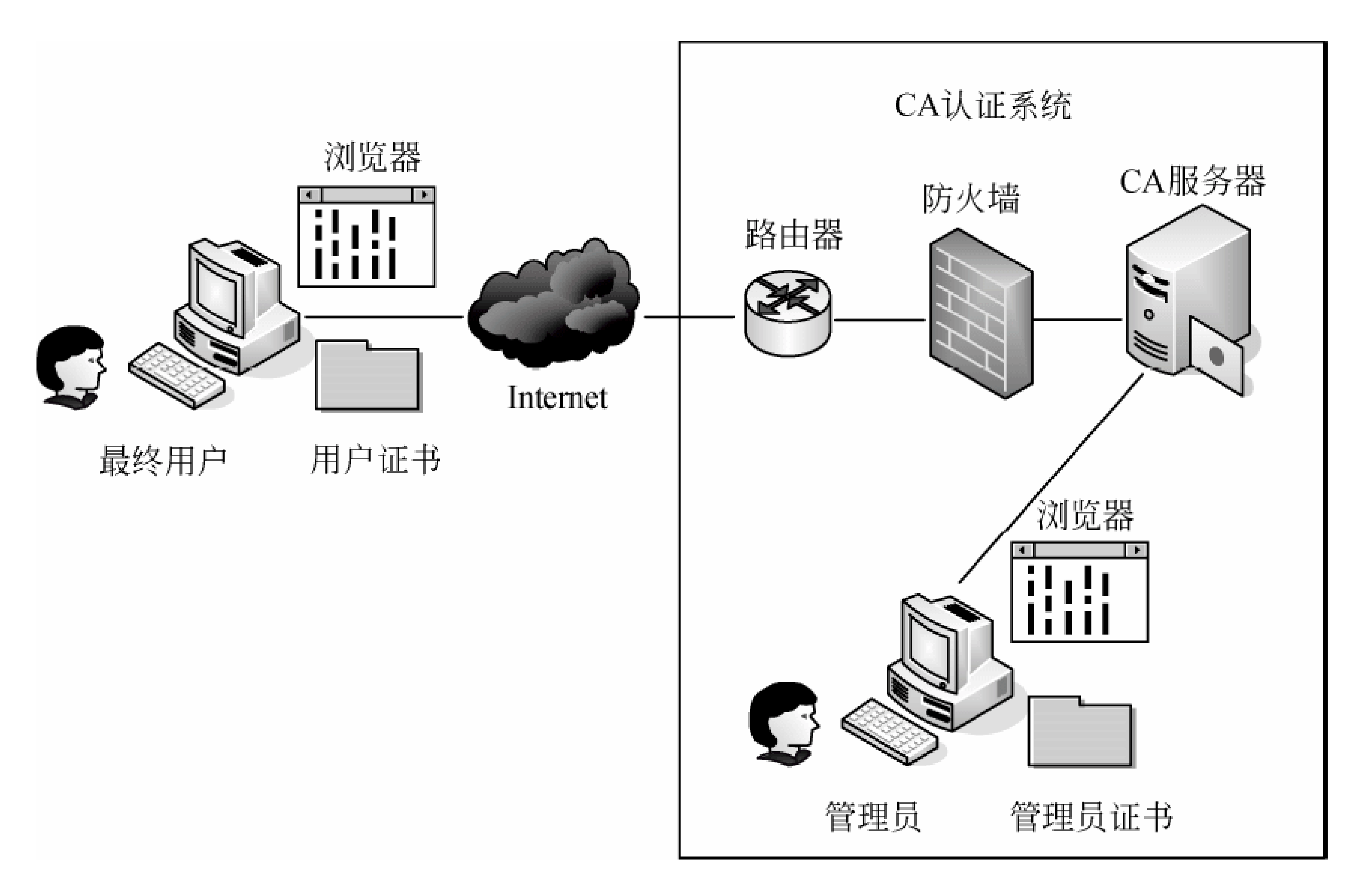


图 2-10　数字证书工作原理

2.5.2　数字证书的颁发机制

1. 颁发过程

数字证书颁发过程一般为：用户首先产生自己的密钥对，并将公钥及部分个人身份信息传送给认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实由用户发送而来，然后，认证中心将发给用户一个数字证书，该证书内包含用户的个人信息和公钥信息，同时还附有认证中心的签名信息。用户就可以使用自己的数字证书进行相关的各种活动。数字证书由独立的证书发行机构发布。数字证书各不相同，每种证书可提供不同级别的可信度。可以从证书发行机构获得数字证书。

2. 授权机构

用户和服务器发布数字证书时，需要选择可信的第三方 CA（Certificate Authority），并遵循一定的程序。CA 中心，即证书授证中心，作为受信任的第三方，承担公钥体系中公钥的合法性验证的责任。CA 中心依据 X.509 标准为每个使用公钥的用户发放一个数字证书，证书包含 X.509 版本号、证书序列号、数字签名的生成算法、证书所有者姓名、证书所有者公钥、颁发者姓名（CA）、证书生效时间、证书过期时间等信息。最后，CA 使用自己的私钥对以上信息进行签名，产生用户的数字证书。数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA 中心的数字签名使得攻击者不能伪造和篡改证书。CA 中心负责产生、分配并管理所有参与网上交易的个体所需的数字证书，因此是安全网上交易的核心过程。数字证书授权机构如图 2-11 所示。

为保证用户之间在网上传递信息的安全性、真实性、可靠性、完整性和不可抵赖性，不仅需要对用户的身份真实性进行验证，还需要有一个具有权威性、公正性、唯一性的

机构，负责向电子商务的各个主体颁发并管理符合国内、国际安全电子交易协议标准的电子商务安全证书。

根据各种不同情况，数字证书可能是 CA 给用户颁发的，或者是用户主动申请的。目前比较常见的国际权威的数字证书颁发认证机构有 VeriSign、GeoTrust 等。在中国，每个省、直辖市设置有国家权威的数字证书颁发机构，比如北京市数字证书认证中心等。但是这种数字证书一般都是收取用户昂贵的申请和维护费用的，所以也有免费的数字证书颁发国际组织，比如 CAcert。随着用户群的增大和颁发手段的可信性，这种免费的数字证书可信度也越来越高。

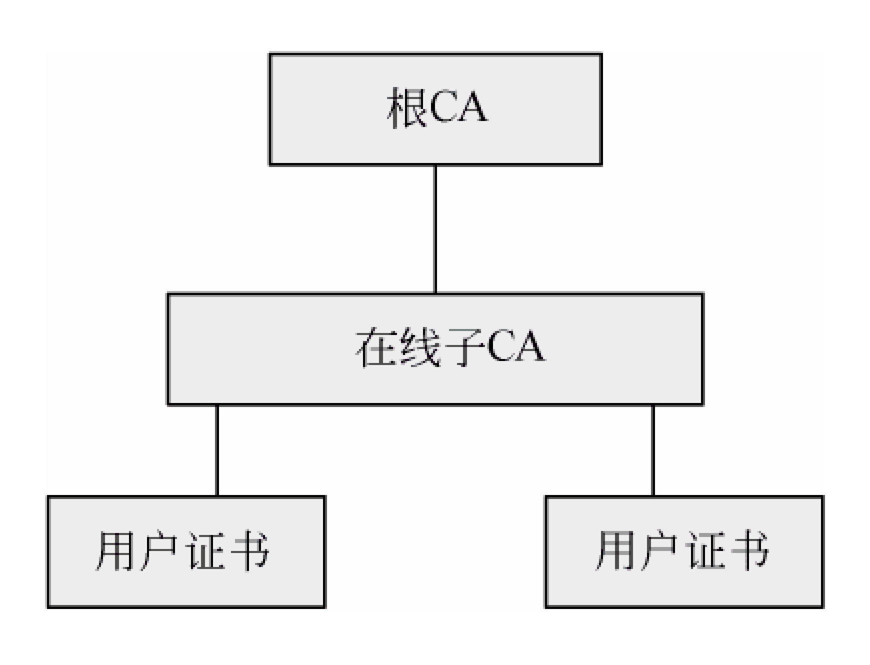


图 2-11　数字证书授权机构

在获得数字证书后，可以将其可保存在电脑里，也可以保存在 IC 卡或 USB Key 中。

2.5.3　数字证书的分类

根据数字证书的应用分类，数字证书可以分为电子邮件证书、服务器证书和客户端个人证书。

1. 电子邮件证书

电子邮件证书的作用是证明邮件发件人的真实性，但是，它并不证明数字证书所有者姓名（由证书上面 CN 一项所标识）的真实性，而只能证明邮件地址的真实性。

当收到具有有效数字签名的电子邮件时，收件者除了能相信该电子邮件确实由某个指定的邮箱发出以外，还可以确信该邮件从发出到接收者接收的过程中没有被第三方篡改过。 此外，运用接收的邮件证书，还可以向接收方发送加密邮件，使得该加密邮件可以在非安全的网络中传输，而只有接收方的证书持有者才可能打开该电子邮件。

2. 服务器证书（SSL 证书）

服务器证书被安装在服务器设备上，其作用是证明服务器的身份和进行通信加密。

在服务器上安装服务器证书后，客户端浏览器可以与服务器证书建立 SSL 连接（建立一条 SSL 安全通道），在 SSL 连接上传输的任何数据都会被加密，可以防止数据信息的泄露。同时，浏览器会自动验证服务器证书是否有效，验证所访问的站点是否是假冒站点（因此，服务器证书也可以用来防止钓鱼站点的欺骗），服务器证书保护的站点多被用来进行密码登录、订单处理、网上银行交易等。目前，全球知名的服务器证书品牌主要有 Verisign、Globlesign、Thawte 和 Geotrust 等。

SSL 证书主要用于服务器（应用）的数据传输链路加密和身份认证，绑定网站域名，不同的产品对于不同价值的数据和要求不同的身份认证。最新的高端 SSL 证书产品是 Extended Validation SSL Certificates，即扩展验证（EV）SSL 证书。在 IE7.0、FireFox3.0、Opera 9.5 等新一代高安全浏览器下，使用扩展验证 VeriSign（EV）SSL 证书的网站的浏览器地址栏会自动呈现绿色，从而清晰地告诉用户正在访问的网站是经过严格认证的，从而最大限度地保护用户上网安全，不给钓鱼网站可乘之机。

3. 客户端个人证书

客户端证书的作用主要是用来进行身份验证和数字签名。

安全的客户端证书一般存储于专用的 USB key 中，且存储于 key 中的证书不能被导出或复制，在使用时则需要输入 key 的保护密码。使用该客户端证书时不仅需要物理上获得其存储介质 USB key，而且还需要知道 key 的保护密码，因此，这也被称为双因子认证。到目前为止，这种认证手段是因特网上最安全的身份认证手段之一。key 的种类较多，常见的有普通 USB key、指纹识别、语音报读、第三键确认、带显示屏的专用 USB key 等。

从广义上来说，目前的数字证书也可分为个人数字证书、单位数字证书、单位员工数字证书、服务器证书、表单签名证书、代码签名证书、WAP 证书和 VPN 证书等。

2.6 信息隐藏技术

随着互联网的迅速发展，网络服务形式越来越丰富，人们可以通过互联网发布自己的作品、重要信息等，同时随之而来的侵权问题也十分严重。如何在充分利用互联网的同时有效地保护知识产权已受到高度重视。信息隐藏技术作为网络安全技术的重要新兴课题，在现代网络环境中保护信息安全起到了重要的作用。信息隐藏通过将信息隐藏到特定的载体中达到不可见的效果，来实现信息的保密传播。信息隐藏的应用非常广泛，包括信息隐写、数字水印等。

2.6.1 信息隐藏

信息隐藏技术是利用载体信息的冗余性，将秘密信息隐藏于普通信息中，使其对非授权者不可见，从而安全地传输信息的技术。信息隐藏技术能够获得更大的隐蔽性和安全性。事实上，信息隐藏的历史非常悠久。在古希腊战争中，为了安全传递情报，奴隶主将奴隶的头发剃光然后情报信息刻在奴隶的头皮上，等奴隶的头发长出来后，再派他去传递情报。这体现的就是信息隐藏的思想。

图 2-12 给出了信息隐藏的过程。在发送方，利用信息隐藏算法，将秘密消息 m 隐藏到载体对象 C 当中，得到伪装对象 C'，然后在不安全的信道中传输 C'。在接收方，利用消息提取算法，从伪装对象 C'中提取出秘密消息 m。在整个传输过程中，秘密消息 m 对攻击者是不可见的。

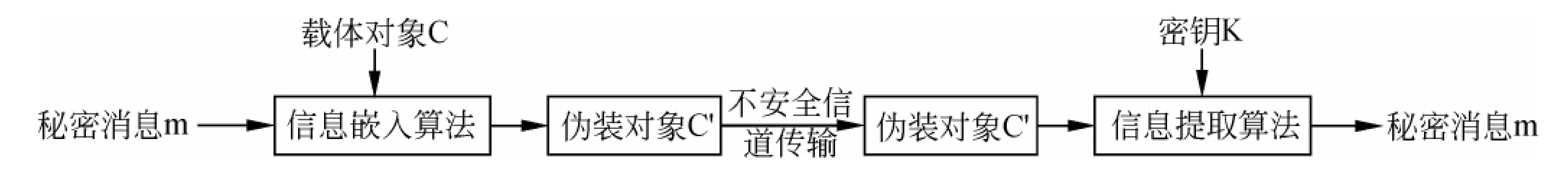


图 2-12 信息隐藏原理图

如图 2-13 所示：将一段文本信息嵌入到一张 JPEG 格式图片中。其中，文本信息就是秘密消息，而 JPEG 图像即为载体对象。在不使用工具进行分析时，载体对象和伪装

对象在人们的视觉中并没有区别。伪装对象在信道中进行传输，在传输的过程中，有可能会遭到攻击者的攻击。提取过程则是在提取密钥的参与下从所接收到的伪装对象中提取出秘密消息，如将上述文本信息从 JPEG 图像中提取出来。

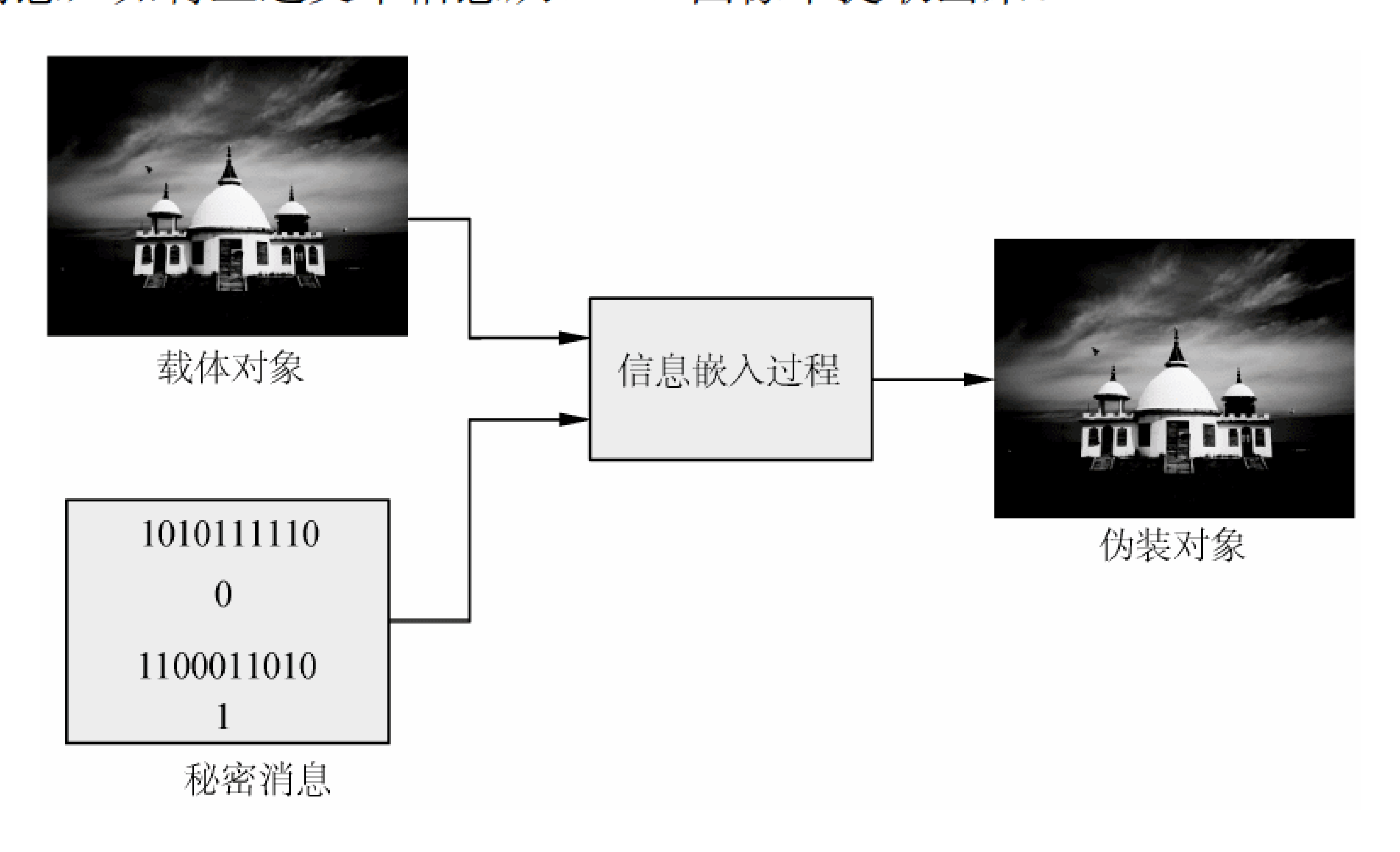


图 2-13　把信息隐藏在图片中

2.6.2　数字水印

数字水印技术是信息隐藏技术的一个重要分支。由于数字作品具有无失真传播复制及易修改、易发表的特点，数字作品的侵权问题日益严重。而数字水印（Digital Watermarking）技术的发展在一定程度上解决了这个问题。数字水印将一些标识信息（即数字水印）嵌入数字载体当中（包括多媒体、文档、软件等）达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。但是，数字水印并不影响原载体的使用价值，也不容易被探知和再次修改。图 2-14 给出了浮现式数字水印的实例，图片中心显示“Brian Kell 2006”的字样。



图 2-14　数字水印实例

1．数字水印的特点

作为数字水印技术基本上具有下面几个方面的特点。

- **安全性**　数字水印的信息应是安全的，难以篡改或伪造，同时，应当有较低的误检测率，当原内容发生变化时，数字水印应当发生变化，从而可以检测原始数据的变更；当然数字水印同样对重复添加有很强的抵抗性。
- **隐蔽性**　数字水印应是不可知觉的，而且应不影响被保护数据的正常使用，不

会降质。

- **鲁棒性** 是指在经历多种无意或有意的信号处理过程后，数字水印仍能保持部分完整性并能被准确鉴别。主要用于版权保护的数字水印易损水印（Fragile Watermarking），和完整性保护，这种水印同样是在内容数据中嵌入不可见的信息。当内容发生改变时，这些水印信息会发生相应的改变，从而可以鉴定原始数据是否被篡改。
- **水印容量** 是指载体在不发生形变的前提下可嵌入的水印信息量。

2. 数字水印算法

一般而言，图像水印技术是通过更改图像中的数据来嵌入水印，其算法上有两个主要的领域。

（1）空间域（时间域）法

早期的图像水印研究主要是发展在空间域中，以灰度图像而言，每个取样点（pixel）一般是以8个位来表示，且由最高有效位（MSB）开始向右排列至最低有效位（LSB），表示数据位的重要性次序，因此可通过更改每个取样点中敏感度最低的LSB来嵌入水印信息，使得水印具有较高的隐密性，这是信息隐藏技术中最常被用来藏入信息的一个既简单又容易实现的方法。但其缺点是容易被攻击者破坏，且难以抵抗噪声、压缩处理、图像处理以及剪切处理等各种攻击。

（2）变换域法

在频域中的水印主要是原始图像转换到频域里，再加入水印数据，将水印嵌入至不同频率成份信号可满足不同需求，当嵌入至高频信号，比较不容易被人眼视觉系统所察觉，嵌入至低频成份信号，由于能量较高因而不容易被破坏。变换域法主要有以下两种常见方法。

第一种是离散余弦转换域法。离散余弦转换是静态图像压缩技术（如JPEG）以及动态视频压缩技术（如MPEG）中的主要核心，而从图像以8*8的像素区块为单位来做离散余弦转换，转换后仍然以8*8的区块大小来表示频率信息，其目的主要是将区块中各个像素的关系性打散，使得大部分的能量可以集中在少数几个基底函数上。

第二种是小波域法。离散小波转换也是一种可将图像的空间域信息转换为频率域信息的技术，其优点除了可以有效地将图像中各个像素的关系性打散之外，还提供了多重分辨率与多频率的特性，使得在处理声音、图像以及视频等信息时的弹性较大，因此近年来被广泛地应用在图像处理、数据压缩以及信息隐藏等研究领域。而离散小波转换则可通过相对应的滤波器而分别作用在图像信息中的列与行来实现。

2.6.3 数字隐写

信息隐藏的另一个重要分支就是数字隐写。隐写就是将秘密信息隐藏到看上去普通的信息（如数字图像）中进行传送，以达到保密传送信息的目的。

数字隐写和数字水印有一定的联系又有一定的区别。二者都是将一个文件隐写至另一个文件中，但使用目的与处理算法不同。隐写侧重将秘密文件隐藏，而水印则较重视

著作权的声明与维护，防止多媒体作品被非法复制等。隐写一旦被识破，则秘密文件十分容易被读取，相反，水印并不侧重隐写文件的隐蔽性，而更在乎增加鲁棒性。

有很多不同的信息隐写方法，其中大部分可看作是替换系统。这些方法尽量把信号的冗余部分替换成秘密信息。根据对载体文件的修改方式，可以把信息隐藏方法分为以下几类。

- **替换系统** 用秘密信息替代载体文件的冗余部分。
- **变换域技术** 在信号的变换域嵌入秘密信息。
- **扩展频谱技术** 采用扩频通信的思想进行信息隐藏。
- **统计方法** 通过更改载体文件的若干统计特性来对信息进行编码，并在提取过程中采用假设检验的方法。
- **失真技术** 通过信号失真来保存信息，在解码时测量与原始载体的偏差。

载体文件相对隐秘文件的大小（指数据含量，以比特计）越大，隐藏后者就越加容易。因为这个原因，数字图像（包含有大量的数据）在因特网和其他传媒上被广泛用于隐藏消息。

2.7 邮件加密软件 PGP

PGP 是基于 RSA 公钥加密体系的邮件加密软件，使用 RSA 和传统对称加密算法的杂合算法，可以对邮件加密，还可以对邮件进行数字签名使收信人确信邮件的发送者。PGP 使用了审慎的密钥管理手段，使得用户事先不需要任何保密的渠道来传递密钥，就可以进行安全通信了。

除了邮件加密与身份确认功能之外，PGP 的功能还包括：资料公钥和私钥加密，硬盘及移动盘全盘密码保护，网络共享资料加密，PGP 自解压文档创建，资料安全擦除等众多功能。

PGP 开发之初是免费的，现在用于商业用途的高级版本是需要收费的。PGP 6.5 版是免费版，在 www.pgp.com 上就可以下载。

2.7.1 PGP 加密原理

邮件加密软件 PGP 充分利用了对称密码速度快和非对称密码安全性高的优势，对邮件进行加密时，同时使用了 RSA 算法和 IDEA 算法（注：IDEA 是一种对称密码算法）。每次加密邮件时，PGP 随机生成一个用于加密邮件内容的 IDEA 密钥，然后用 RSA 公钥对该密钥加密。这样收件人收到邮件之后，先用 RSA 密钥解密出这个随机密钥，再用 IDEA 解密邮件本身。这样的加密就做到了既有 RSA 体系的保密性，又有 IDEA 算法的快捷性。PGP 加密原理如图 2-15 所示。

2.7.2 PGP 安装

PGP 安装只需按提示完成即可。在图 2-16 中可以选择要安装的组件，选择 PGP

Microsoft Outlook Express Plugin 复选框，就可以在 Outlook Express 中直接用 PGP 加密邮件对邮件进行签名。

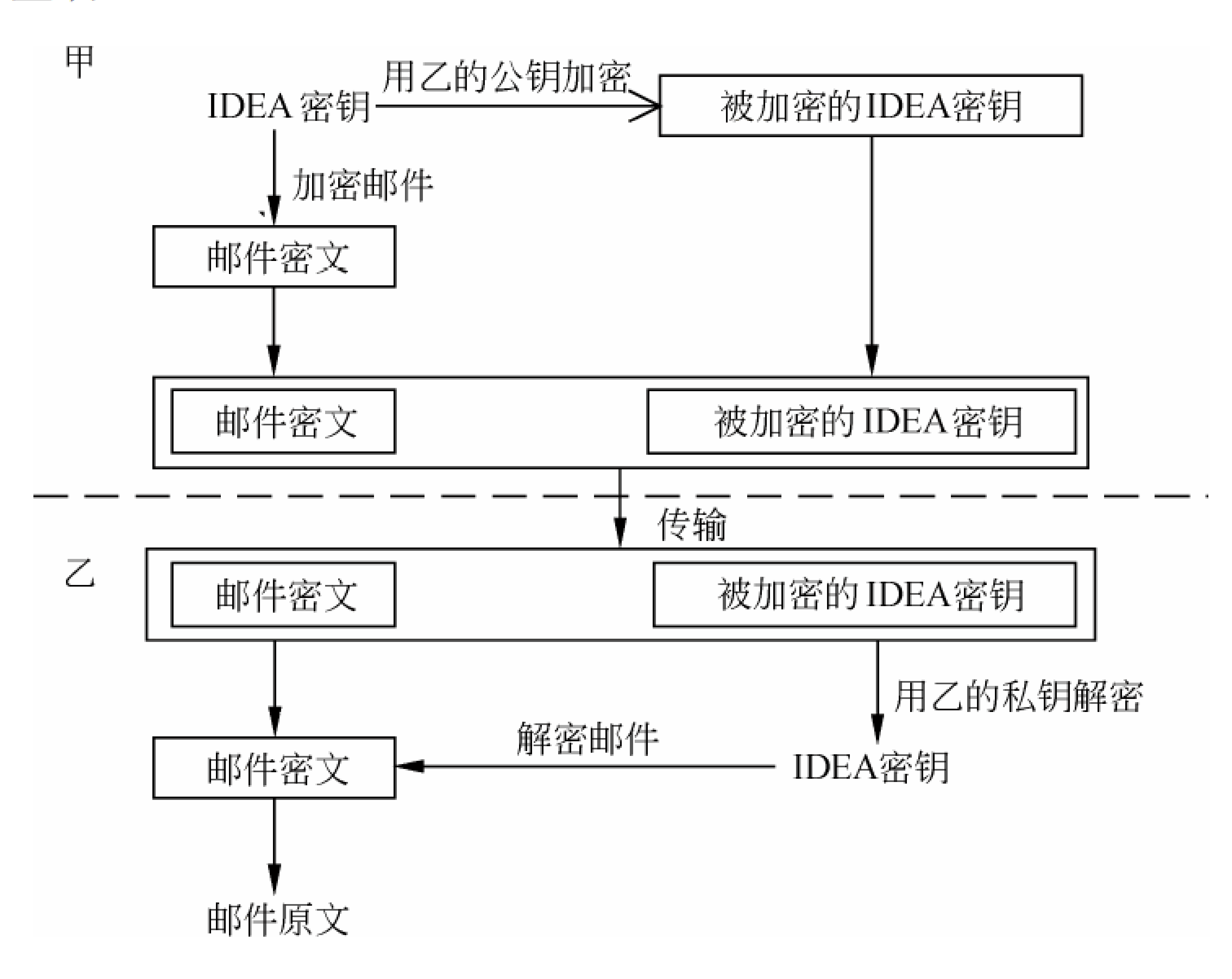


图 2-15　PGP 加密原理图

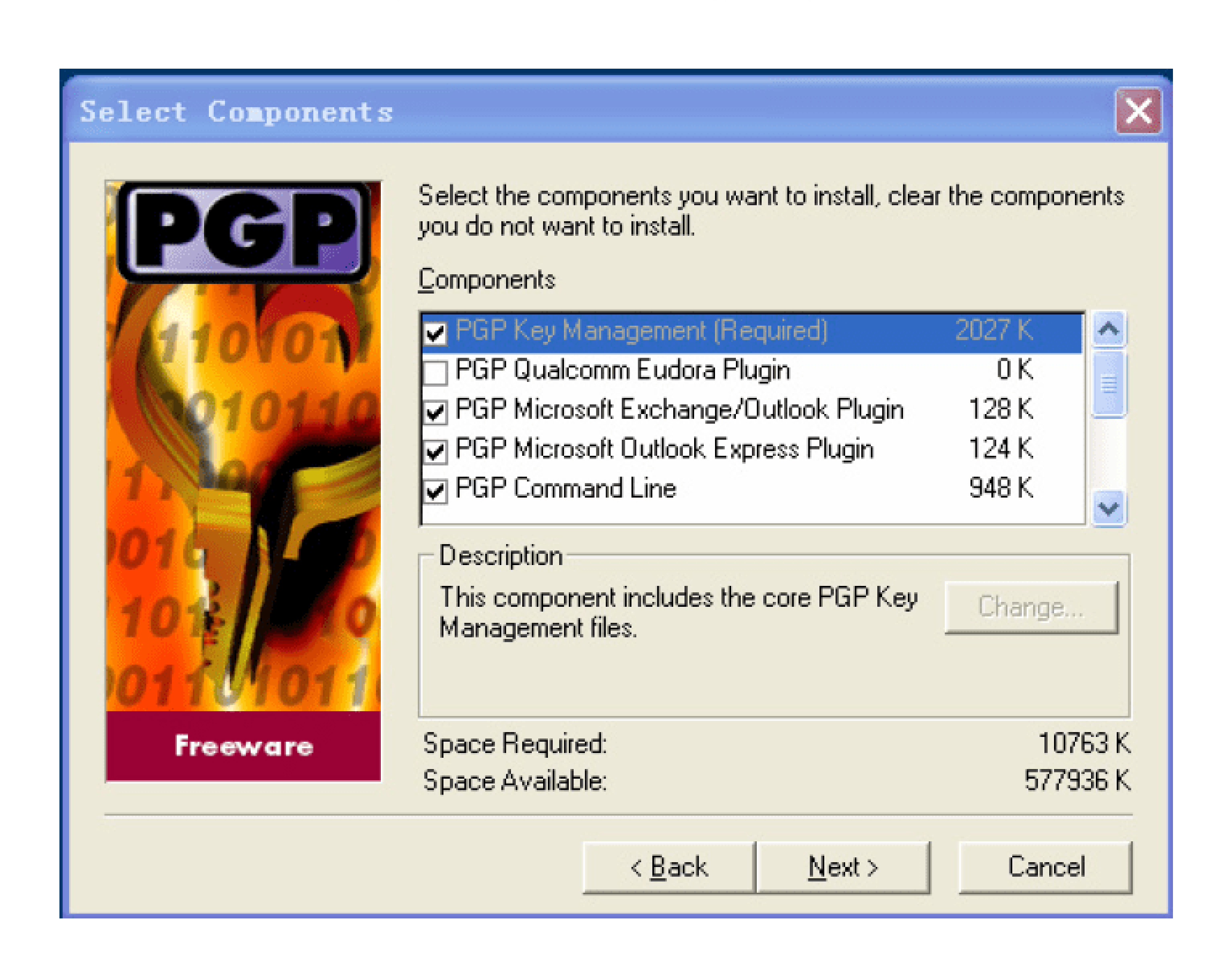


图 2-16　PGP 安装示意图

2.7.3　PGP 生成密钥

单击“开始”→PGP 命令会看到如图 2-17 所示的画面。图中存储了一系列用户的密钥对。

单击图标或者 Keys→New Key 命令开始生成密钥。PGP 有一个很好的密钥生成向导，只要按照提示步骤操作即可。（在安装软件时，同样会提示是否生成密钥。）

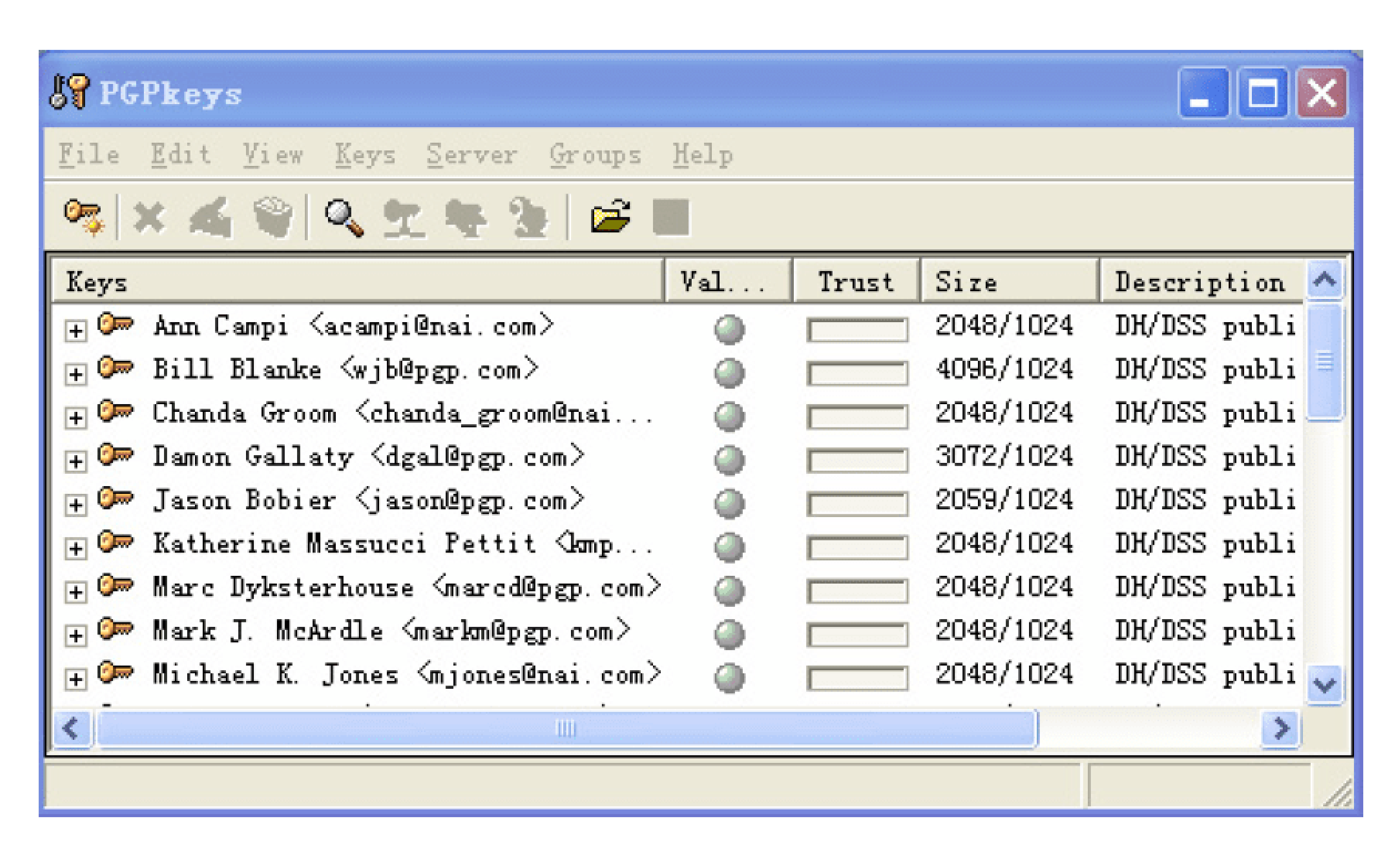


图 2-17　PGP 生成密钥示意图

PGP 同时生成了一对密钥，其中一个是公钥，可以分发给其他用户，用于加密文件，另一个是私钥，由用户自己保存，用于解密加密文件。

第一步，PGP 提示这个向导的目的是生成一对密钥，可以用它来加密文件或对数字文件进行签名。单击 next 按钮即可。

第二步，输入全名和邮件地址，如图 2-18 所示。

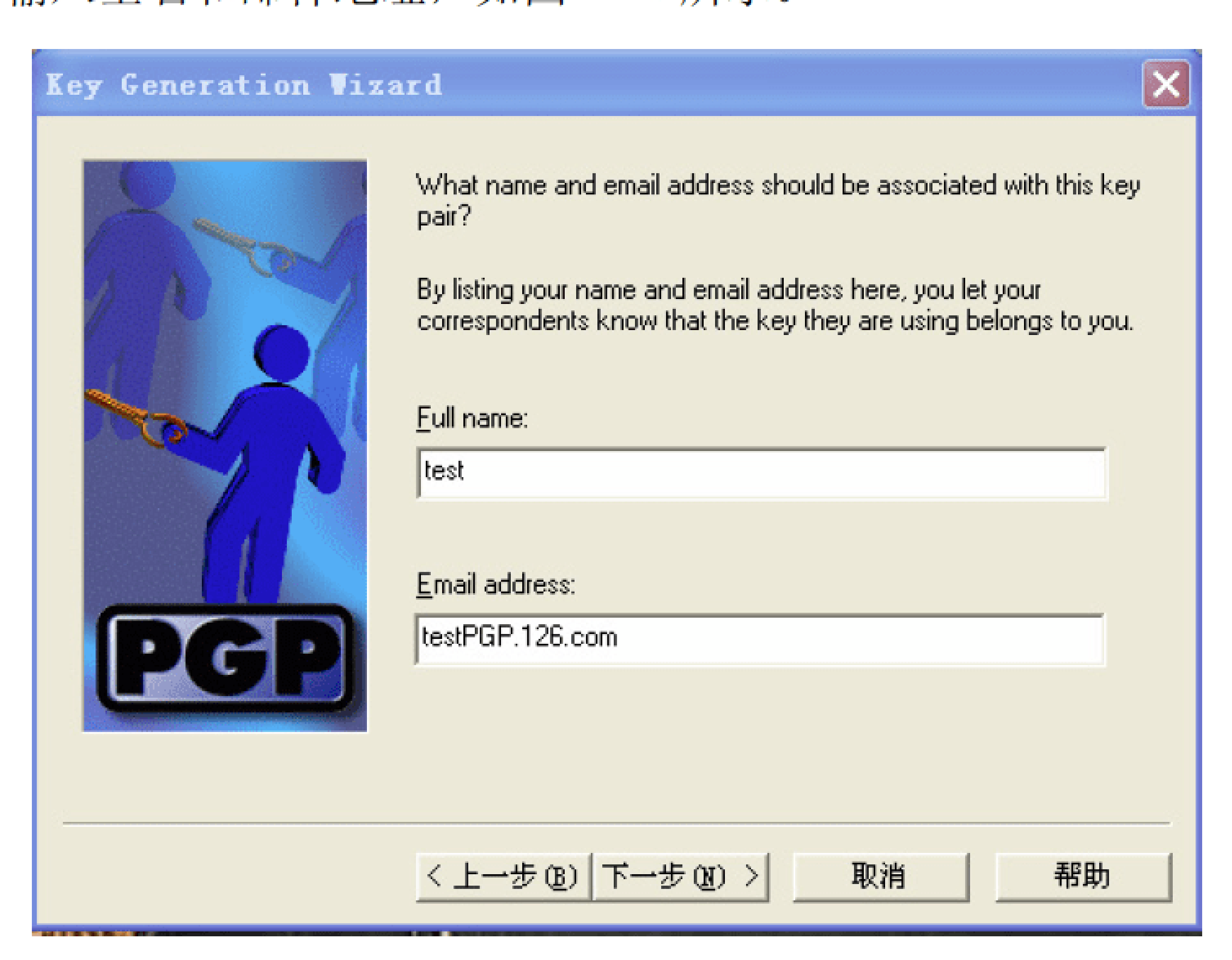


图 2-18　输入用户名和邮件地址

第三步，选择加密类型，如图 2-19 所示。PGP 5.0 以前的版本多用 RSA 加密方式，5.0 以后多选用 Diffie-Hellman/DSS。

第四步，指定密钥长度。通常来说密钥位数越大被解密的可能性越小，就越安全，但是在执行解密和加密时会需要更多的时间，所以一般选择 2048 位即可。

第五步，PGP 询问密钥的过期日期，可以选择从不过期或指定一个日期作为过期的

界限。

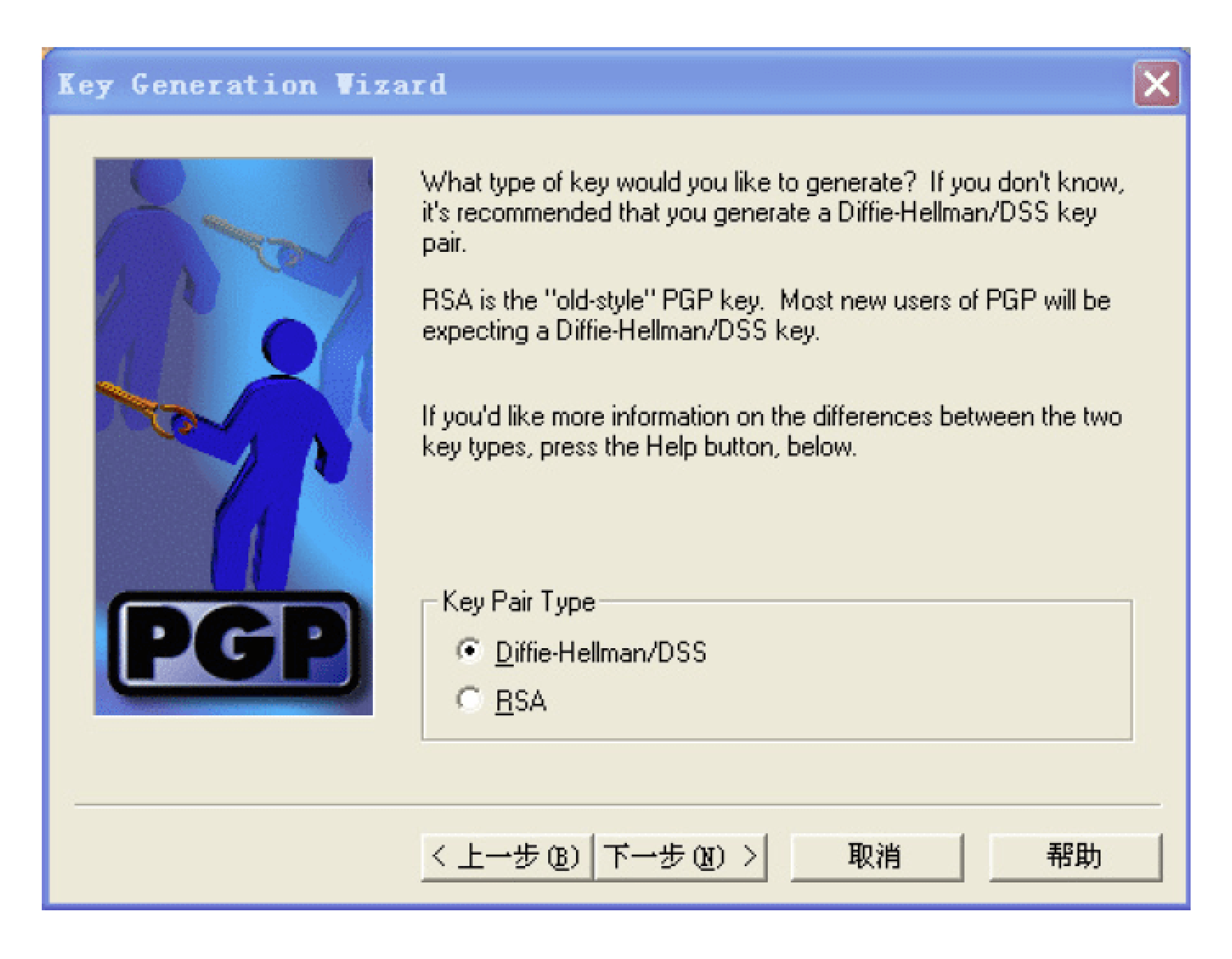


图 2-19　选择加密类型

第六步，设置口令，如图 2-20 所示。这个口令用于私钥的保密，提供了更强的安全性。建议设置的口令大于 8 位，并且最好包括大小写、空格、数字、标点符号等。另外，PGP 支持中文作为口令。边上的 Hide Typing 复选框指示是否显示输入的口令值。



图 2-20　设置口令

第七步，PGP 花费一些时间生成密钥，如图 2-21 所示，然后询问是否想把生成的公共密钥发送到服务器上去。这个服务器是 PGP 公司提供的一个免费密钥服务器，用来进行方便的公钥验证/发布/自动搜索加密等功能。例如某个用户的公钥已经上传到了该服务器，那么给这个用户发送加密邮件时，便不需要要求对方单独发一次密钥来导入，PGP 内置功能会自动连接并完成对应信箱公钥的下载/验证/签名的操作，减少人工干预次数，

提高易用性。不过，为了更加安全，并不建议把密钥上传到服务器上。



图 2-21　PGP 生成密钥

第八步，密钥生成结束。可以看到用户刚生成的密钥被加入到了密钥链表里面，如图 2-22 所示。

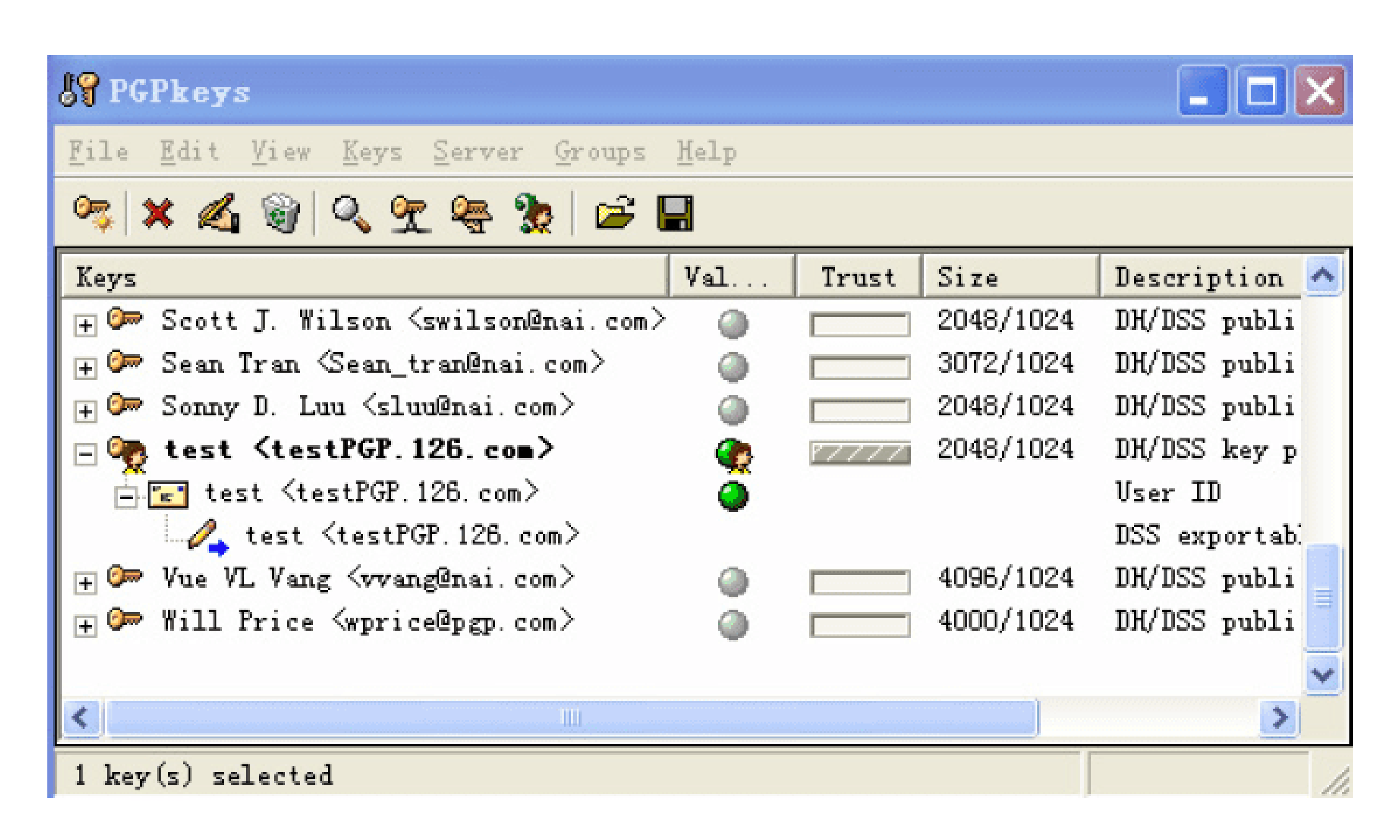


图 2-22　PGP 密钥生成结束

2.7.4　PGP 加解密

对文件加密非常简单，只需选中需要加密的文件，然后右击，在弹出的快捷菜单中选择 PGP→Encrypt 命令。之后，会弹出一个对话框，选择要用来进行加密的密钥，然后双击使它加到下面的 Recipients 列表框中即可，如图 2-23 所示。单击 OK 按钮进行加密，就得到扩展名为“.pgp”的加密文件。

解密时双击扩展名为“.pgp”的文件或选中文件并右击，在弹出的快捷菜单中选择 PGP→Decrypt 命令，在图 2-24 中的下面的文本框中输入口令即可。

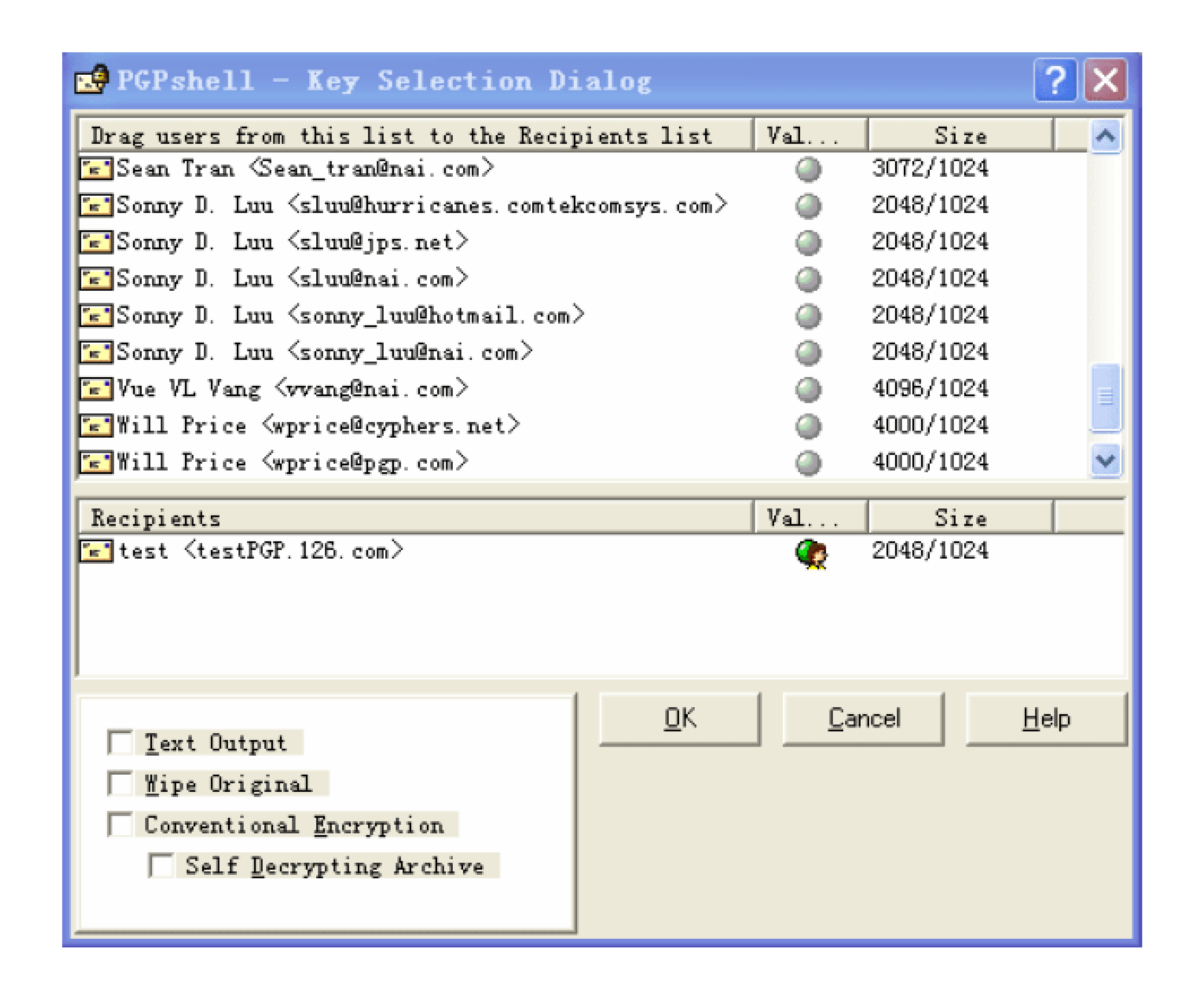


图 2-23　PGP 加密示意图

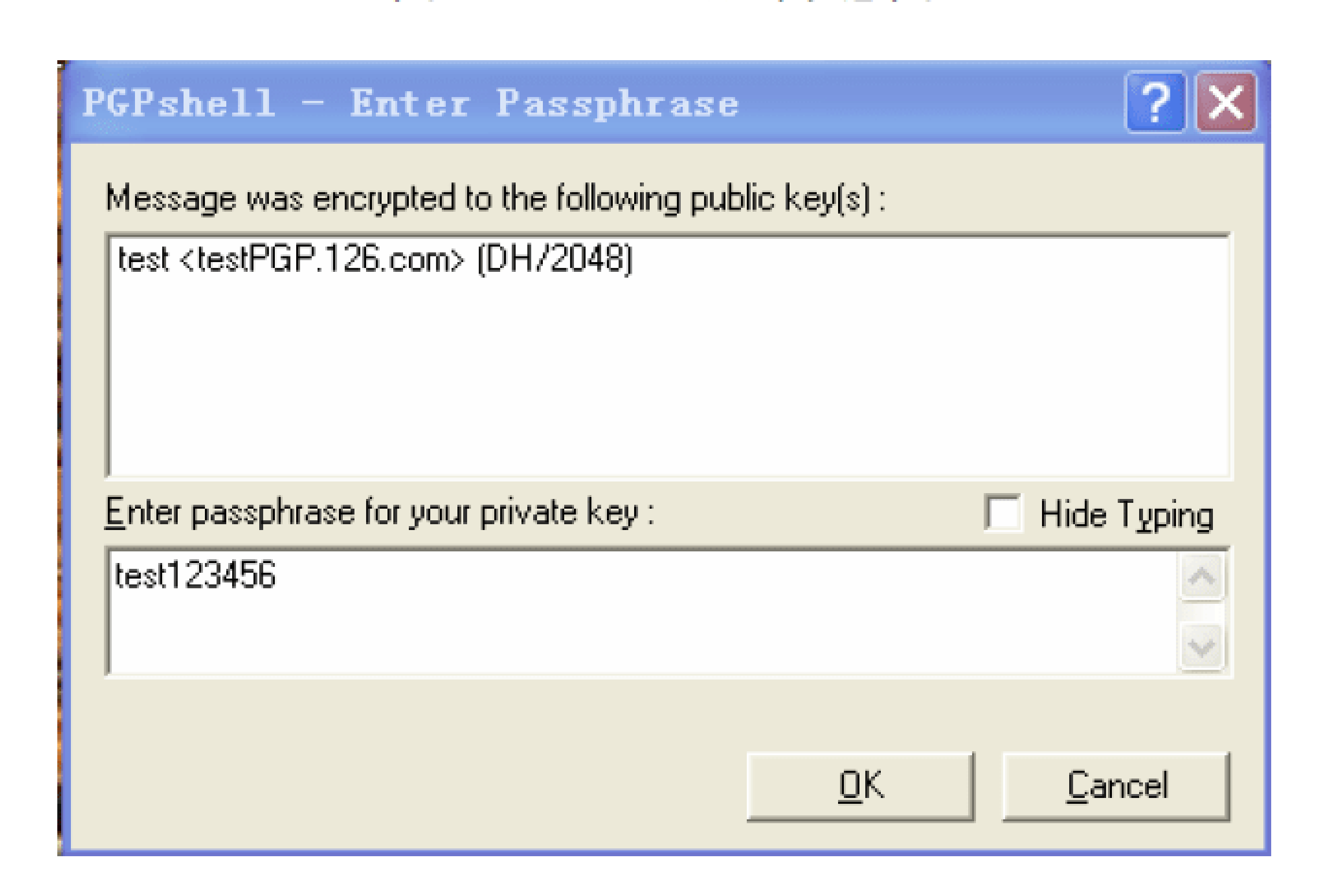


图 2-24　PGP 解密示意图

如果要在 Outlook Express 或 Outlook 中直接对邮件进行加密，可在写新邮件时单击工具栏中的图标 PGP Encrypt，当邮件写完发送时，PGP 会如上所示弹出对话框请求用户选择密钥，同上操作即可。

习　题

一、选择题

1. 密码技术的哪一个目标不能被对称密码技术实现？（　　）

　A. 完整性
　B. 保密性
　C. 不可否认性
　D. 认证性

2. A 想要使用非对称密码系统向 B 发送秘密消息。A 应该使用哪个密钥来加密消息？（　　）

　A. A 的公钥
　B. A 的私钥
　C. B 的公钥
　D. B 的私钥

3. DES 的有效密钥长度是多少？（　　）

　A. 56 比特
　B. 112 比特

C．128 比特
D．168 比特

4．下面哪种情况最适合使用非对称密码系统？（　　）
A．公司电子邮件系统
B．点到点的 VPN 系统
C．证书认证机构
D．Web 站点认证

5．下面哪个哈希函数最适合 8 位处理器？（　　）
A．SHA-256
B．SHA-512
C．MD4
D．MD2

6．Grace 想要使用数字签名技术向 Joe 发送一则消息，为了获得数字签名，她应该对哪种信息进行签名？（　　）
A．明文消息
B．密文消息
C．明文消息摘要
D．密文消息摘要

7．Joe 收到由 Grace 签了名的信息，请问 Joe 该使用哪个密钥来验证签名？（　　）
A．Joe 的公钥
B．Joe 的私钥
C．Grace 的公钥
D．Grace 的私钥

二、问答题

1．密码技术主要有哪些，有哪些应用？
2．简述对称加密和非对称加密的优缺点。
3．描述 RSA 加密的算法过程。
4．描述数字证书的工作原理及分类。

课后实践与思考

一、在网上下载一款 PGP 软件安装在个人主机上，熟悉其使用方法。然后尝试使用 PGP 对个人电脑上的文件进行加密，并尝试在同学之间发送使用 PGP 加密的电子邮件。

二、RADIUS 服务器的配置，如下面实例所示。

试验环境：3 台虚拟机，一台 radius-server，一台 vpn-server，一台远程 client，如图 2-25 所示。

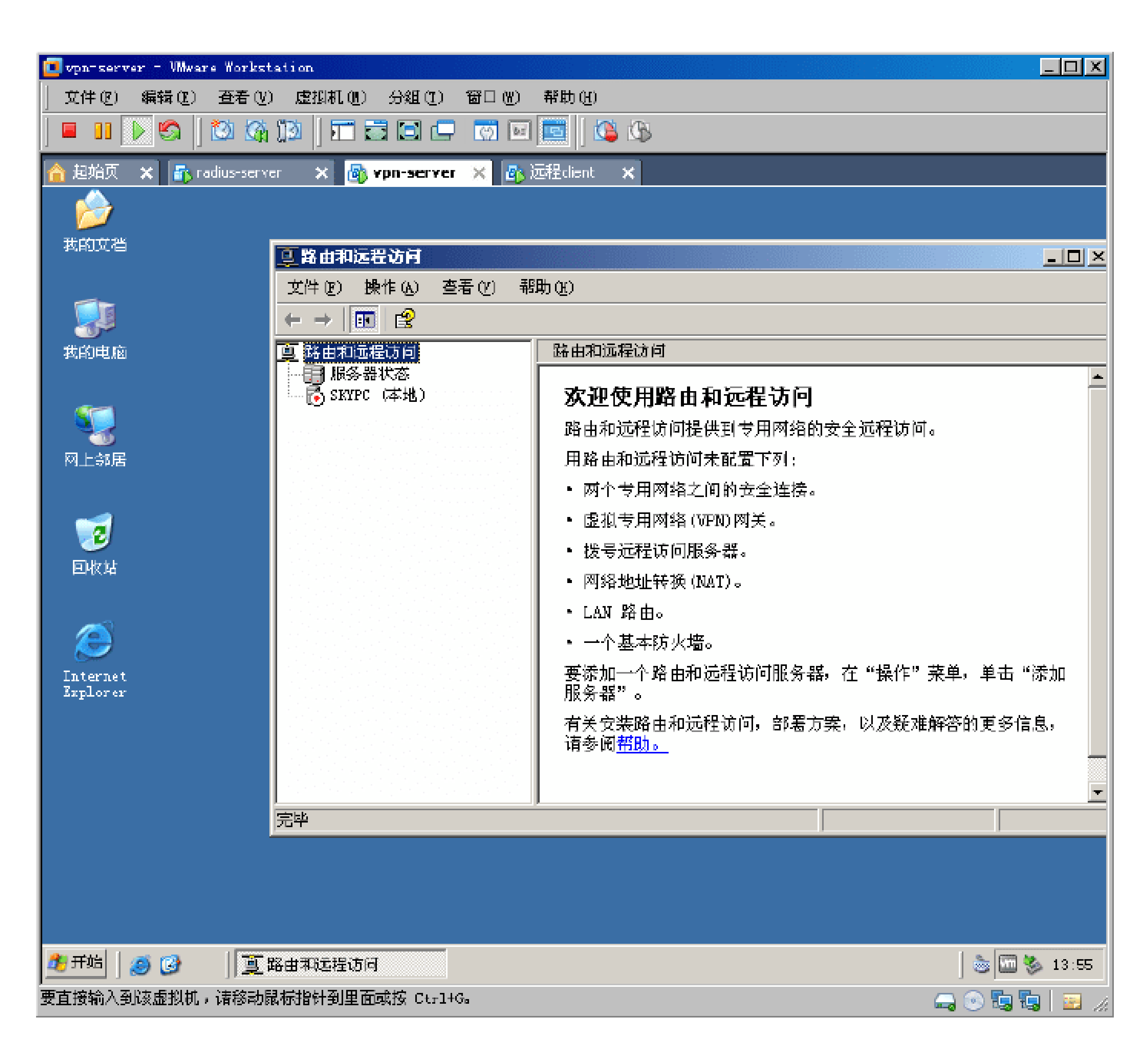


图 2-25　实验环境

（1）配置 vpn-server，连接 radius 的 IP，如图 2-26 所示。



图 2-26　配置 vpn-server

（2）注意，先不连接 RADIUS 服务器，如图 2-27 所示。

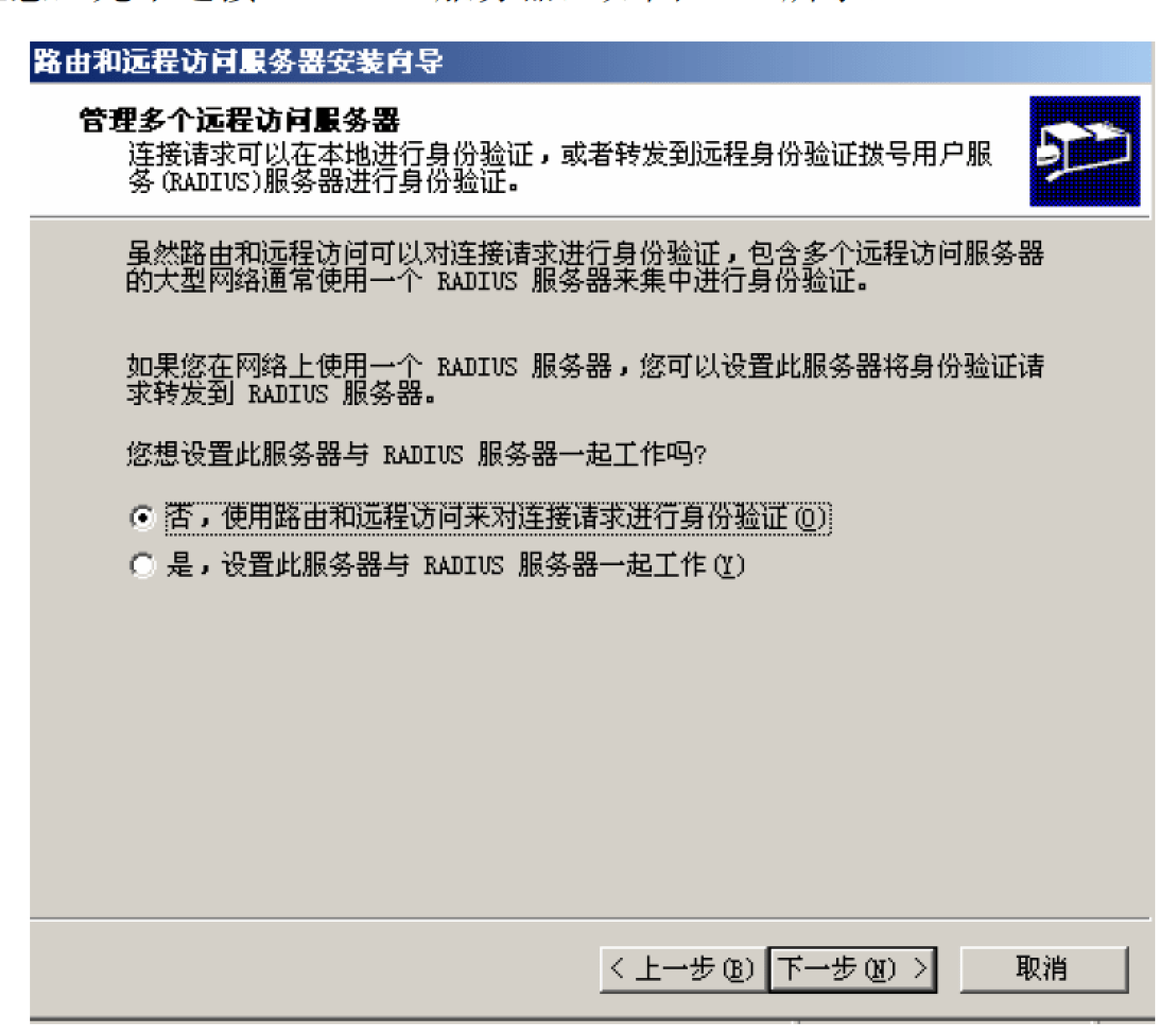


图 2-27　不连接 RADIUS 服务器

（3）使用远程客户端拨号连接到 vpn-server，若成功，说明 vpn-server 配置没问题，如图 2-28 所示。

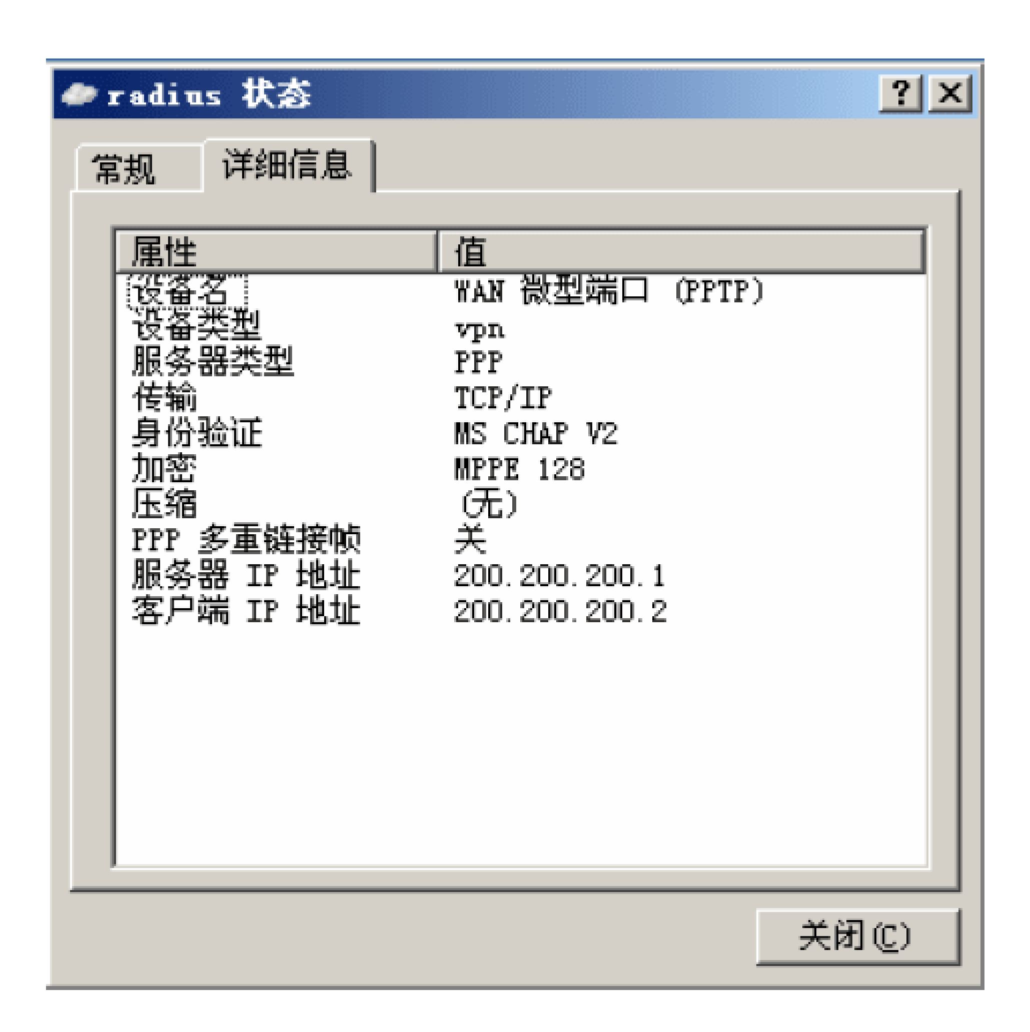


图 2-28　vpn-server 配置成功

（4）改成 RADIUS 身份验证并配置，如图 2-29 所示。

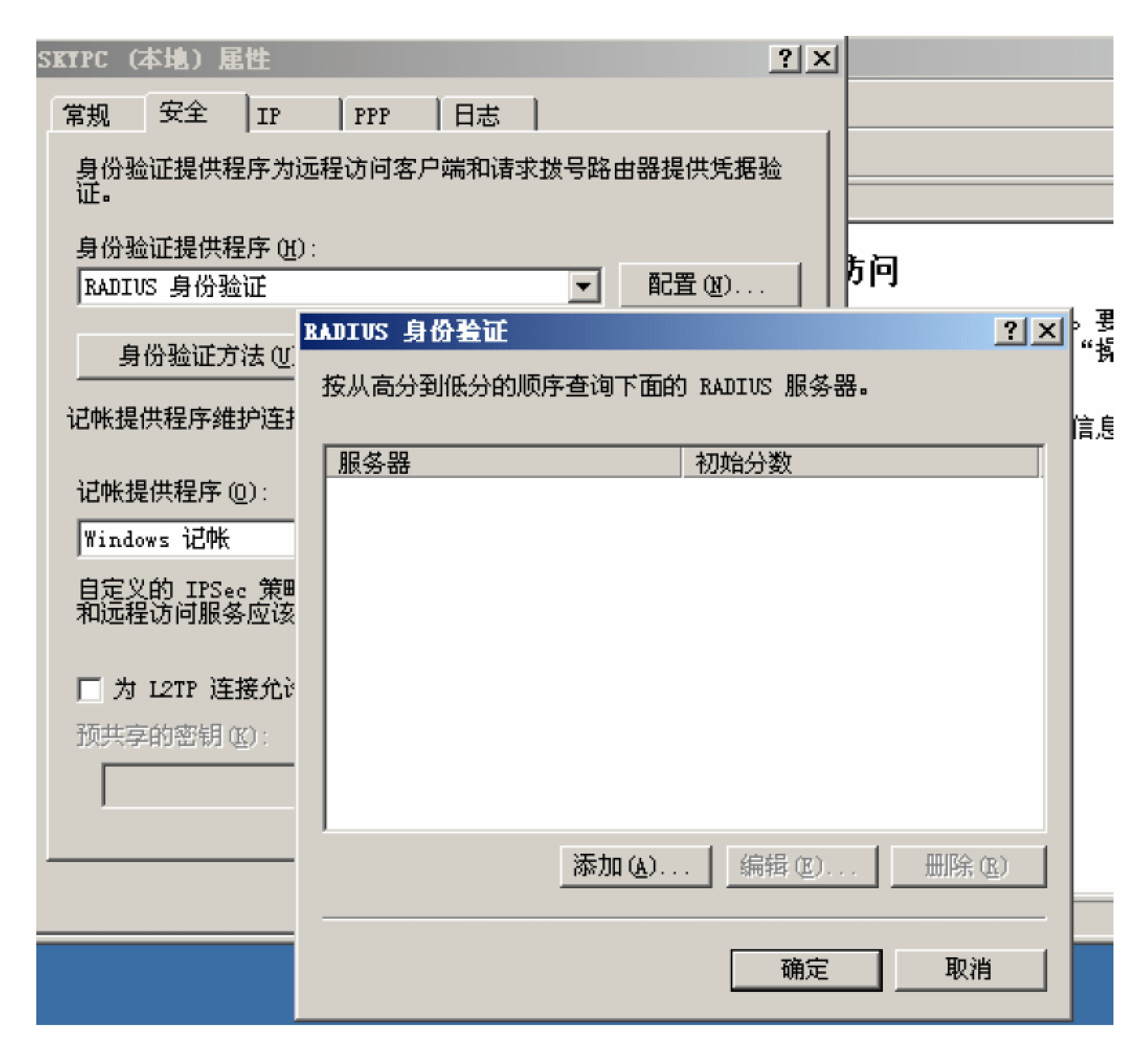


图 2-29　RADIUS 身份验证

（5）添加 RADIUS 服务器地址，如图 2-30 所示。

（6）同样，记账也改成 RADIUS 记账模式，如图 2-31 所示，并输入服务器地址，重启路由远程服务即可

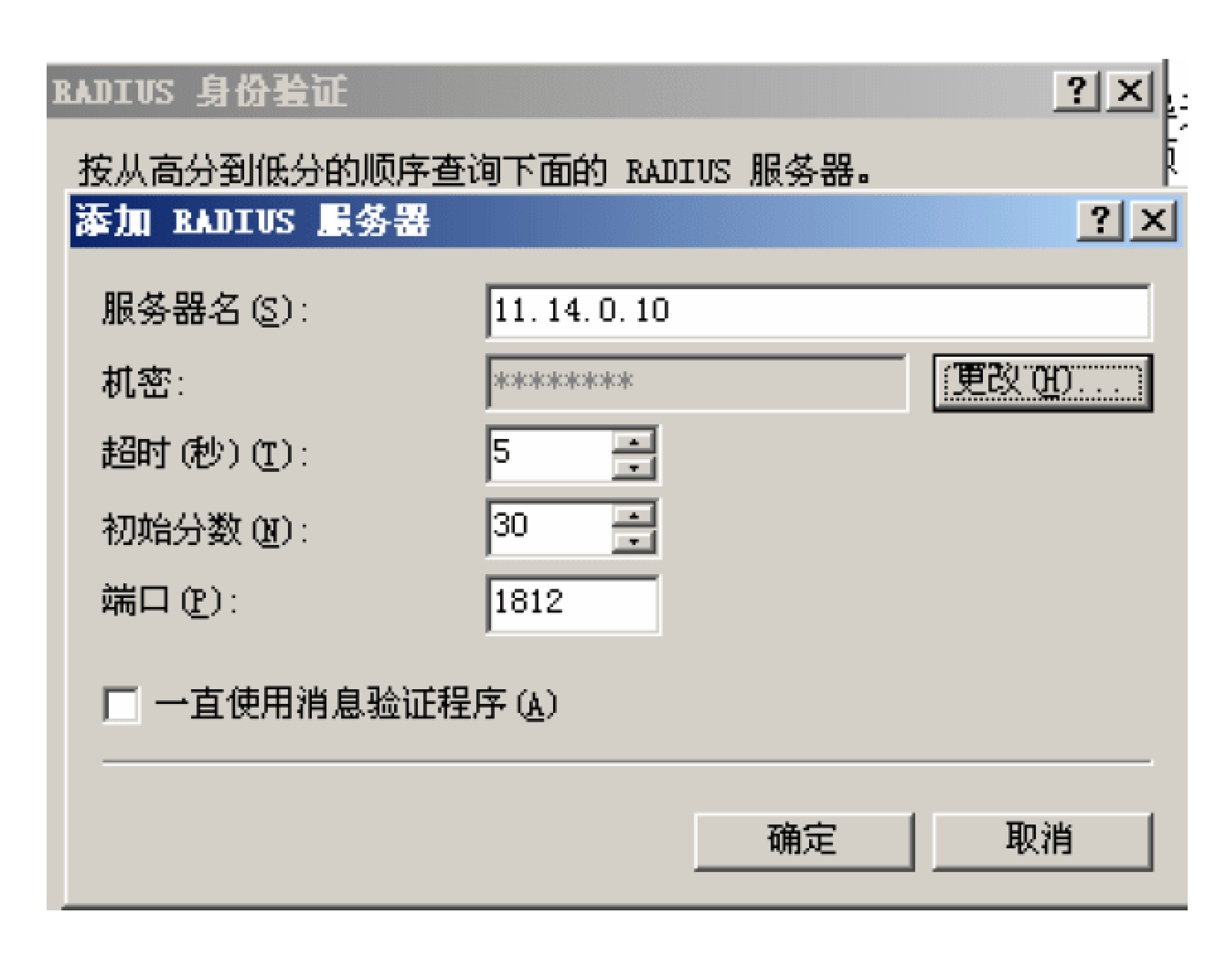


图 2-30　添加 RADIUS 服务器

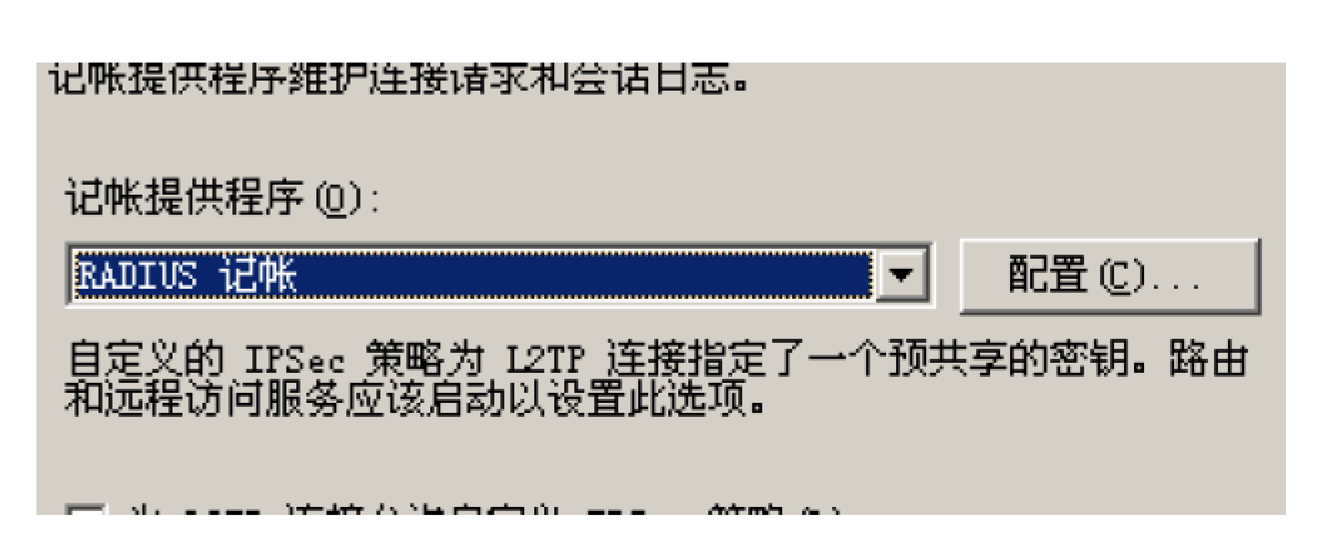


图 2-31　修改记账模式

（7）再到 RADIUS 服务器上配置，安装组件，如图 2-32 所示。

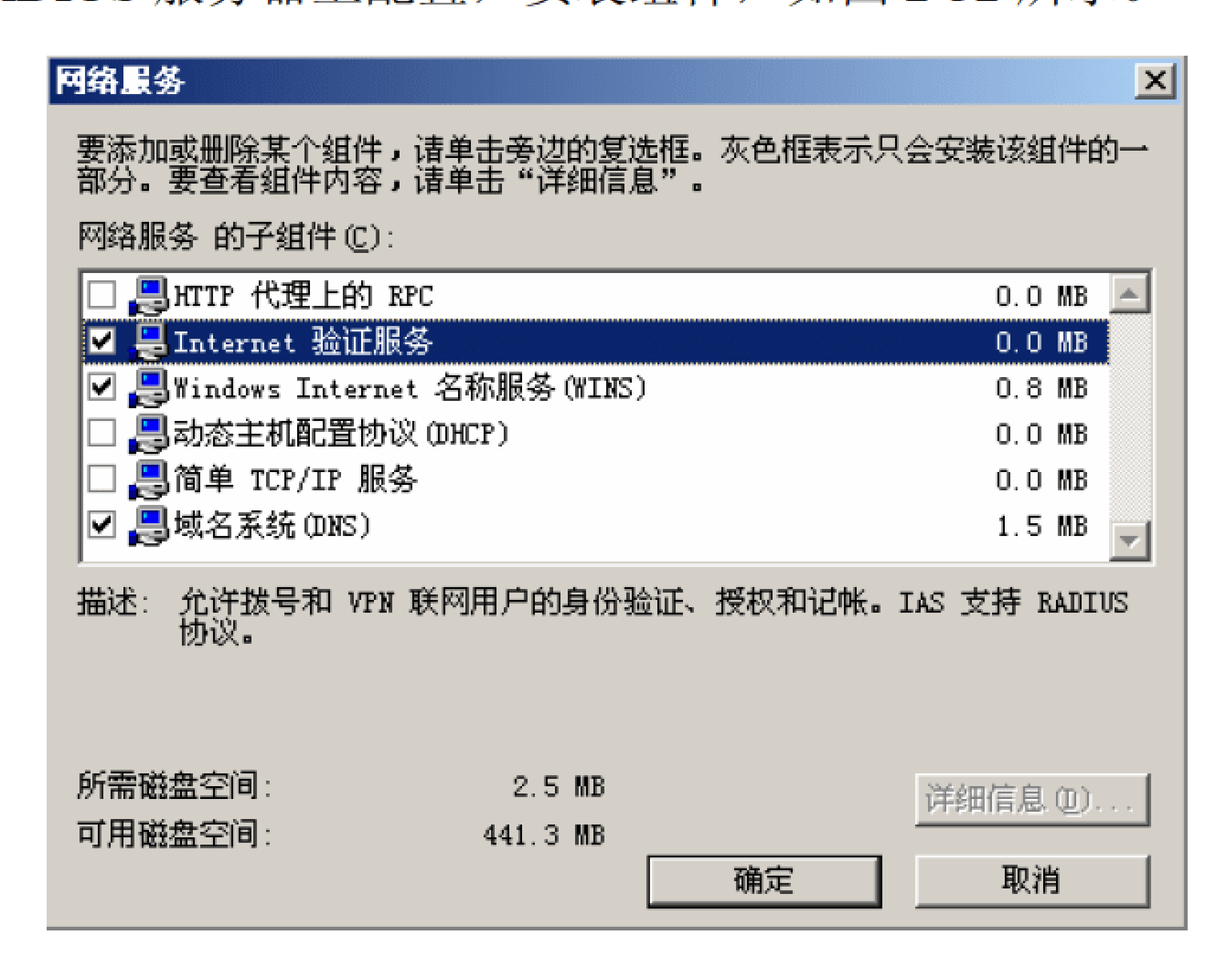


图 2-32　安装组件

（8）在管理工具中打开，新建 RADIUS 客户端，如图 2-33 所示。

（9）输入共享的机密，就是在 vpn 服务器上添加 radius 服务器时输入的机密，如图 2-34 所示。

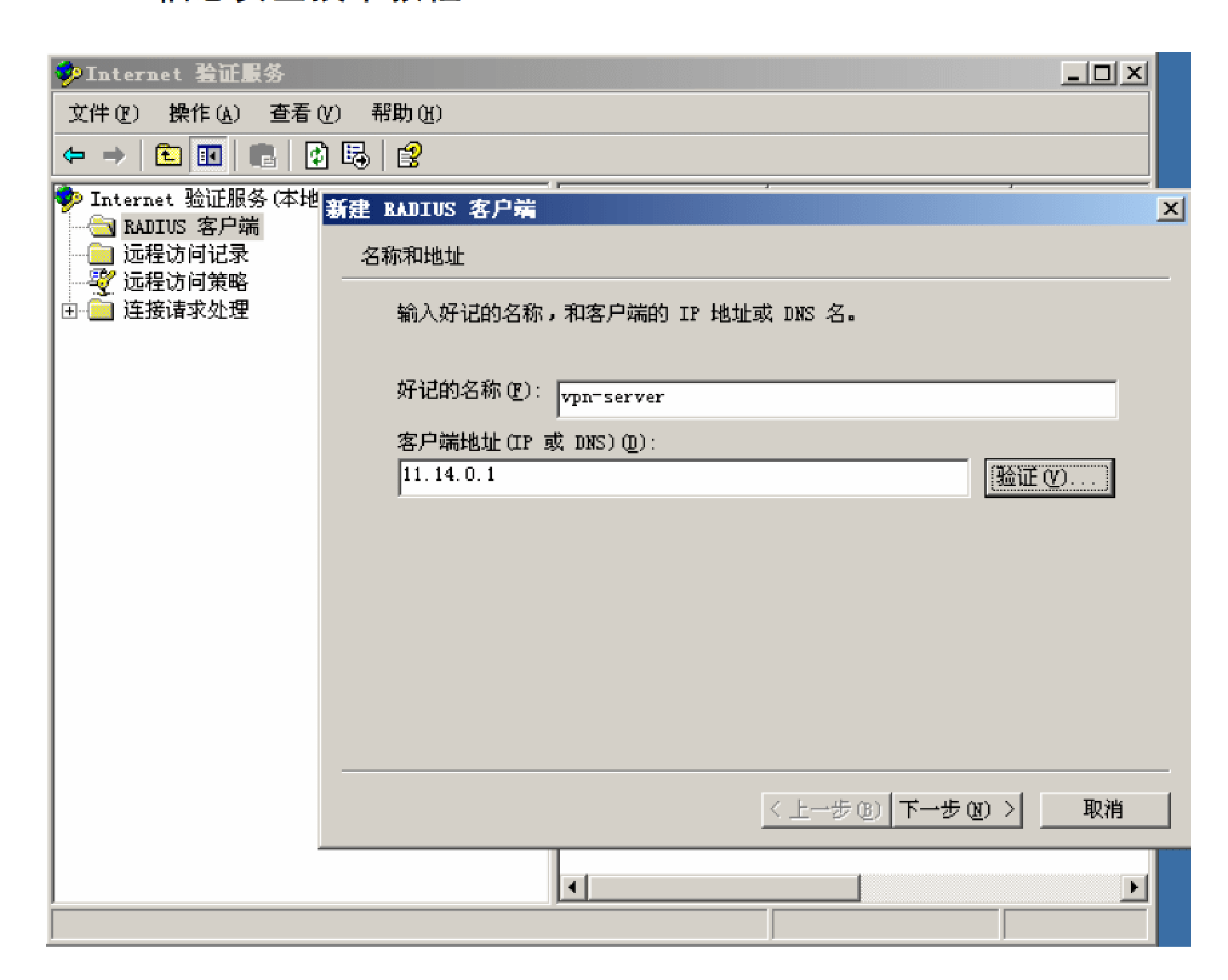


图 2-33 新建 RADIUS 客户端

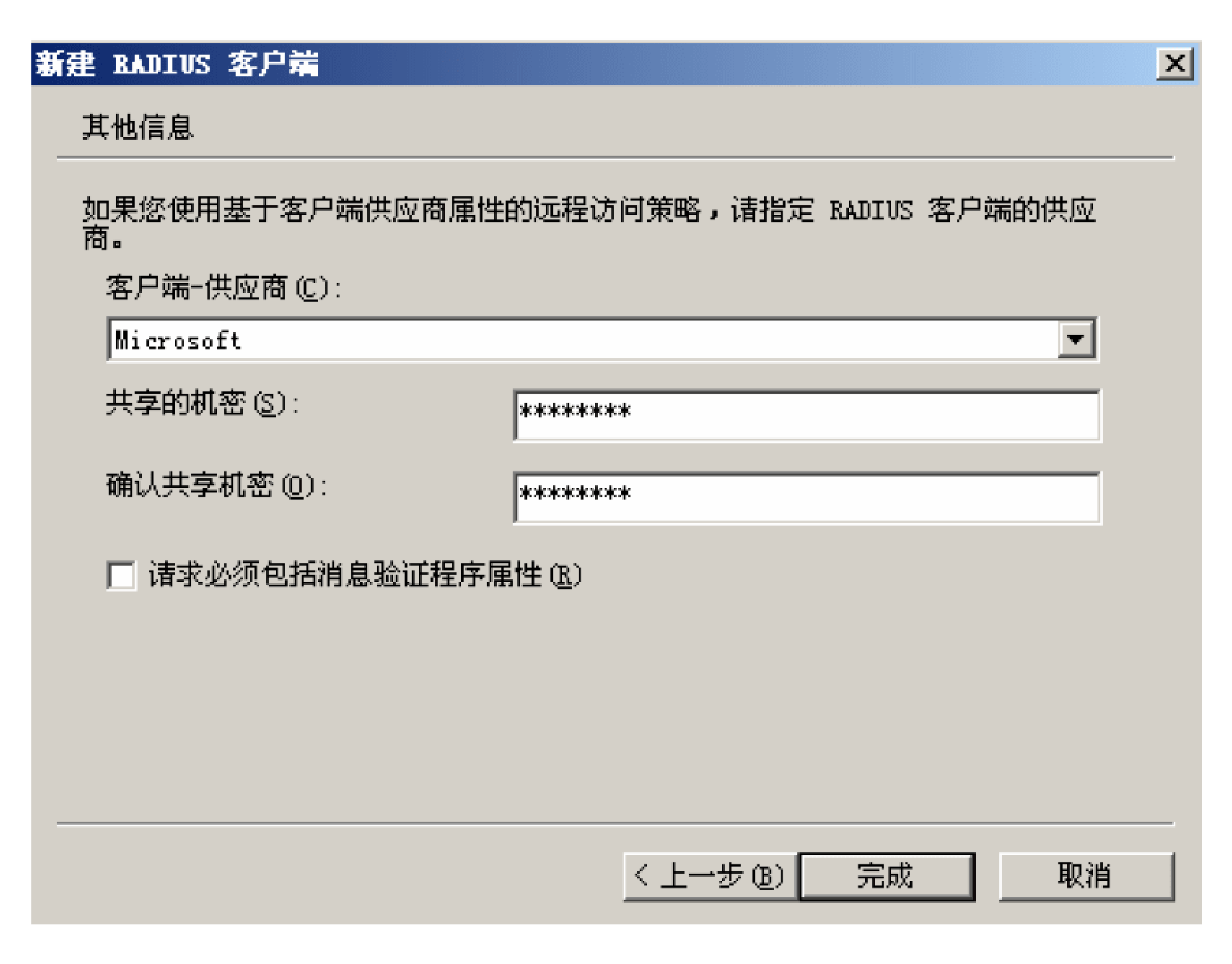


图 2-34 输入共享的机密

（10）选择远程访问记录的设置，如图 2-35 所示。

（11）可以发现远程客户端上 vpn 连接已经断了，如图 2-36 所示。

（12）接下来在 RADIUS 服务器上创建用户，远程客户端使用在 RADIUS 服务器上创建的用户拨号，登录成功，如图 2-37 所示。

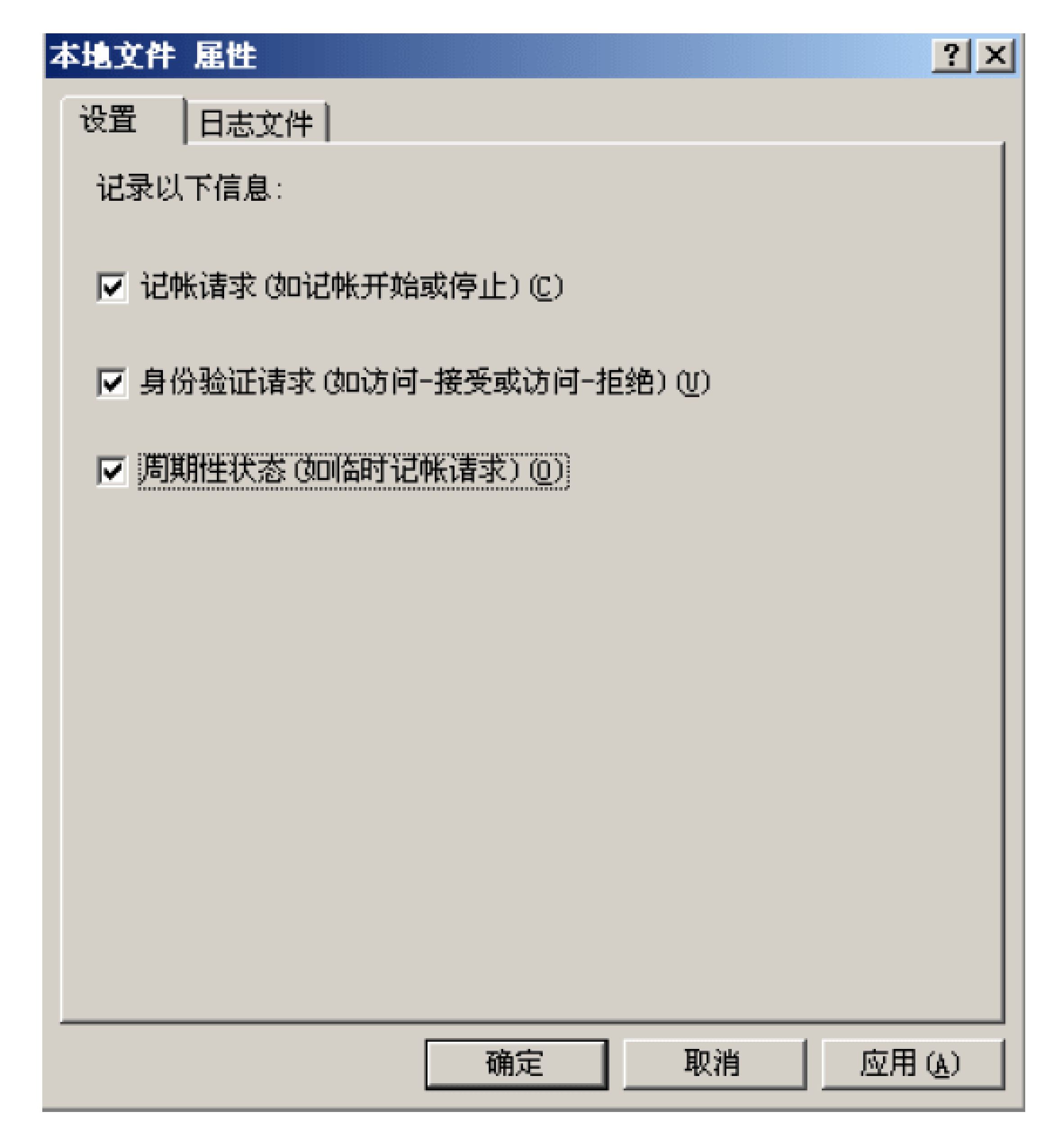


图 2-35　信息记录设置

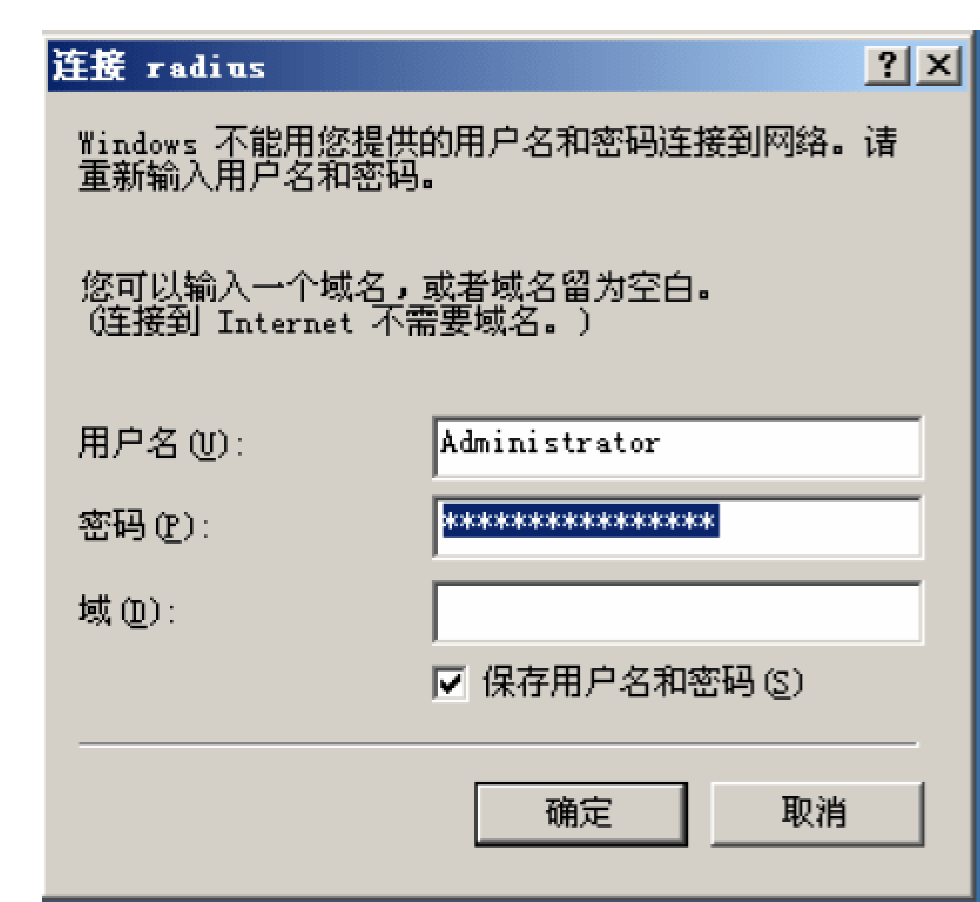


图 2-36　vpn 连接断开



图 2-37　登录成功

（13）查看 radius 服务器记录，如图 2-38 所示。

```
11.14.0.1,jiangjun,12/23/2006,14:33:52,IAS,SKYPC,44,29,4,11.14.0.1,6,2,
11.14.0.1,jiangjun,12/23/2006,14:33:52,IAS,SKYPC,25,311 1 11.14.0.10 12
11.14.0.1,jiangjun,12/23/2006,14:33:54,IAS,SKYPC,40,1,41,0,4,11.14.0.1,
```

图 2-38　radius 服务器记录

第 3 章　认 证 技 术

本章学习重点：

- 认证的基本概念
- 认证所依赖的特殊因子
- 认证的组成部分
- 各种认证技术

3.1 基本概念

认证是验证某个人或系统身份的过程，就是向认证机构提供信息确认某个人或系统是否是其声称的那个人或系统。例如，在私人计算机系统中，认证过程通常是指某个人，使用由系统管理员提供的口令登录。用户持有口令是保证身份真实性的一种手段。

一般而言，认证要求用户出具一定的证据证明自己就是所声明的那个人。这些证据建立在一些独特的认证因子上，这些因子可分为 3 种类型：用户所知道的，用户所拥有的和用户本身特有的。

- **用户所知道的**　指用户心里知道的一些东西。可能是一个口令，或用户和认证者共享的一个机密字。尽管这种方法管理开销较小，但也存在着用户需要记忆大量口令等一系列缺点。用户可以在所有系统上使用同样的口令登录，也可以定期更换口令，显然，第二种方法更值得推荐。基于这种因子的认证实例包括口令、口令句和个人识别号（PINs）。
- **用户所拥有的**　指用户获取的关于身份识别的各种物理实体，如安全内核、动态口令卡、安全暗号或其他任何形式的卡或标签。与上一种形式相比，这种方法更加安全。显然，保存口令卡比记忆一长串的口令更加容易。
- **用户所特有的**　指用户本身特有的生物特征，比如声音、指纹、虹膜等其他一些生物特征。尽管这些生物特征易于使用，但读取生物特征的设备非常昂贵。这方面的应用实例包括指纹、视网膜、DNA 和手掌几何学。

除了这 3 种因子之外，其他一些因子虽然不是直接的，但也在认证中起到了一定的作用。例如用户的位置，通常指用户的物理或逻辑位置。这种方法可以被用在访问某些资源的终端上。

3.2 认证组成

一个认证系统由 5 部分组成：请求认证的用户或工作组，用户或工作组提供的用于认证的特征信息，认证机构，认证机制以及接受或拒绝访问系统资源的访问控制机制。

- **用户或工作组**　指那些想要访问系统资源的用户或工作组。如果是个人用户，

需要向认证机构出示证据来证明确实已被授权访问系统的资源。如果是工作组，也必须向认证机构提供证据证明工作组中的每一个用户成员都被授权访问系统的资源。

- **特征信息** 指用户向认证机构提供的用于认证身份的信息。如前所述，这些信息分为 4 种类型：用户所知道的、用户所拥有的、用户本身特有的和用户的位置。申请访问系统资源的用户或工作组可以使用包含多种不同特征的方法来加强认证，提供更好的安全保证。例如，在网上交易过程中，通常需要用户输入登录口令，并同时出具电子密码卡，确保认证的安全性。
- **认证机构** 指识别用户并指明用户是否被授权访问系统资源的组织或设备。认证机构可以是系统指定的服务器、防火墙、局域网服务器、企业内部专用服务器，也可以是全球身份认证服务器。认证机构通过执行完整的认证机制来认证用户的身份。
- **认证机制** 认证机制由 3 部分组成，分别是输入组件、传输系统和核实器。输入组件是用户和认证系统之间的接口，用于将用户认证信息传输给认证系统。在分布式环境中，输入组件可以是计算机键盘、读卡器、摄影机、电话等类似的设备。传输系统负责在认证系统内部各个组件之间传递信息。核实器是认证过程的关键组件，完成对用户认证信息的分析计算。现代认证系统中，信息在网络上传输，可以利用密码协议进行加密传输，也可直接以明文形式发送。
- **访问控制单元** 用户身份信息经核实器分析计算的结果通过传输系统传输到访问控制单元。在这里，访问控制单元反复核对这些信息与数据库中存储的用户认证信息是否匹配。如果匹配，访问控制系统就颁布一个临时证书批准用户访问所需的系统资源。如果不匹配，就拒绝用户对系统资源的访问。存储用户信息的数据库可能存储在特定的认证服务器上，也可储存在本地介质文件中。

图 3-1 给出了一个完整的认证过程。当用户或工作组申请使用系统资源时，向系统提交身份认证信息，这些信息通过输入组件传输给核实器。核实器对用户的身份认证信息进行分析计算，并将结果传输给访问控制单元。访问控制单元将其与存储在用户数据库中的用户认证信息进行比较，如果匹配，则接受用户的访问请求；如果不匹配，则拒绝用户的访问请求。

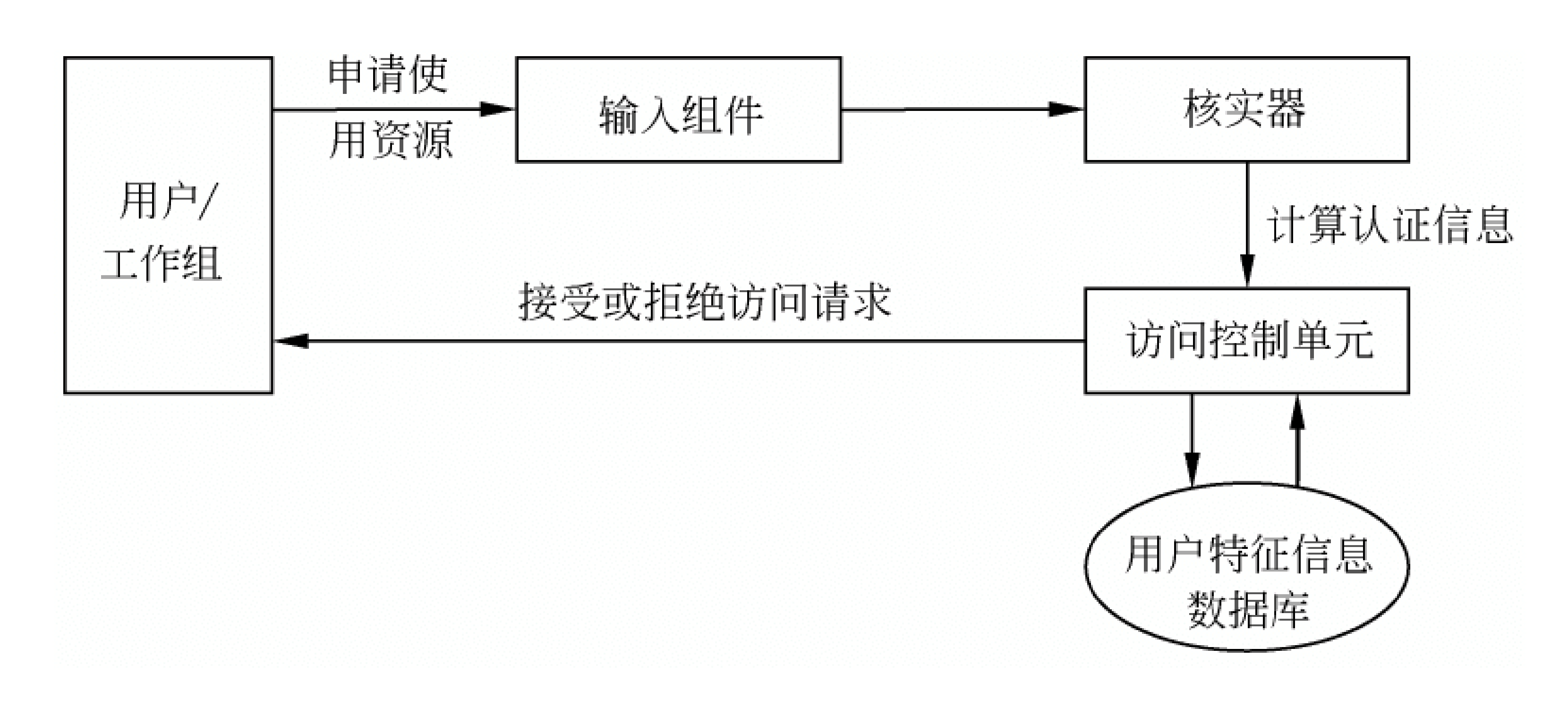


图 3-1 认证过程示意图

3.3 认证技术

随着网络安全技术的不断发展，已经出现了多种不同的认证技术。根据不同的功能水平和安全需要，这些认证技术可以单独使用，也可以同时使用。主要的认证技术包括口令认证、公开密钥认证、远程认证、匿名认证和数字签名认证。

3.3.1 口令认证

口令认证是最古老、最简单的一种认证方法，经常作为系统的默认设置。口令认证包括可重用口令认证、一次性口令认证、挑战应答口令认证和混合口令认证。

1. 可重用口令认证

可重用口令认证有两种类型：用户(user)认证和客户端(client)认证。

- **用户认证** 通常由申请使用系统资源的用户发起。接到用户的资源使用请求后，服务器向用户索要用户名和口令，然后将这些信息和数据库上的信息进行比对，如果匹配成功，用户请求被允许，可以访问系统资源。例如，人们在使用电脑时，需要输入用户名和口令，就是最简单的用户认证。
- **客户端认证** 一般情况下，用户请求服务器的认证，然后被授权使用系统资源。用户通过认证并不意味着可以自由使用任何想要的系统资源。通过认证只是说明用户被授权使用所请求的那些资源，但并不能超过这个限度。这种类型的认证就叫做客户端认证。这种认证根据用户的身份，使用户受限访问系统的资源。

可重用口令认证方法简单、运行速度快、使用广泛，但也存在着一系列的问题。为了避免记忆复杂口令，用户常会选择简单口令，或把口令值记录下来，增加了安全隐患。同时，随着计算机计算水平的提高，通过蛮力攻击能够很容易破解系统的口令值。

2. 一次性口令认证

一次性口令认证也被称为会话认证，认证中的口令只能被使用一次，然后被丢弃，从而减少了口令被破解的可能性。在一次性口令认证中，口令值通常是被加密的，避免明文形式的口令被攻击者截获。最常见的一次性口令认证方案是 S/Key 和 Token 方案。

（1）S/Key 口令

这种口令认证基于 MD4 和 MD5 加密算法产生，采用客户—服务器模式。客户端负责用 hash 函数产生每次登录使用的口令，服务器端负责一次性口令的验证，并支持用户密钥的安全交换。在认证的预处理过程中，服务器将种子以明文形式发送给客户端，客户端将种子和密钥拼接在一起得到 S。然后，客户端对 S 进行 hash 运算得到一系列一次性口令。也就是说，第一次口令是通过对 S 进行 N 次 hash 运算得到，下一次的口令是通过对 S 进行 N–1 次 hash 运算得到。在服务器端保存着用户上一次成功登录的口令值，因此，当用户访问系统时，服务器只需要将本次传输过来的口令进行一次 hash 运算。如果得到结果和存储的值一致，就验证了用户身份的正确性。在产生口令过程中，hash 函

数的使用次数要逐次减 1，因此，过一段时间用户就要重新初始化用于产生口令的密钥、种子以及运算次数 N。S/Key 保护认证系统不受外来的被动攻击，但是无法阻止窃听者对私有数据的访问，无法防范拦截并修改数据包的攻击，无法防范内部攻击。

（2）Token（令牌）口令

这种方法要求在产生口令的时候使用认证令牌。根据令牌产生的不同，又分为两种方式：挑战应答式和时间同步式。

- **挑战应答式**　是一个握手认证的过程。用户持有内置种子密钥和加密算法的令牌。图 3-2 给出了挑战应答式认证的过程。请求使用系统资源的时候，用户需先输入用户名和静态口令，之后服务器会用一个随机数向用户发起挑战。用户将此随机数输入口令令牌卡进行进算，并将得到的应答传送给服务器。服务器使用相同的密钥和算法计算得到应答数，并将其和用户送来的应答数进行比较。如果相同，则允许用户访问系统资源。在分布式系统中，挑战应答认证方式得到广泛的应用。但是，这种认证方式也存在着一些问题，包括用户交互问题及易受到试错求解法的攻击。对于服务器的挑战，用户必须做出快速反应。如果超过时间限制，请求就会被拒绝。某些情况下，用户还需要记住较长的应答，也很容易出错。在试错攻击法中，攻击者不断尝试应答值来登录系统。在给定的时间帧中，利用功能强大的计算机设备来自动产生应答，很可能碰到正确应答。

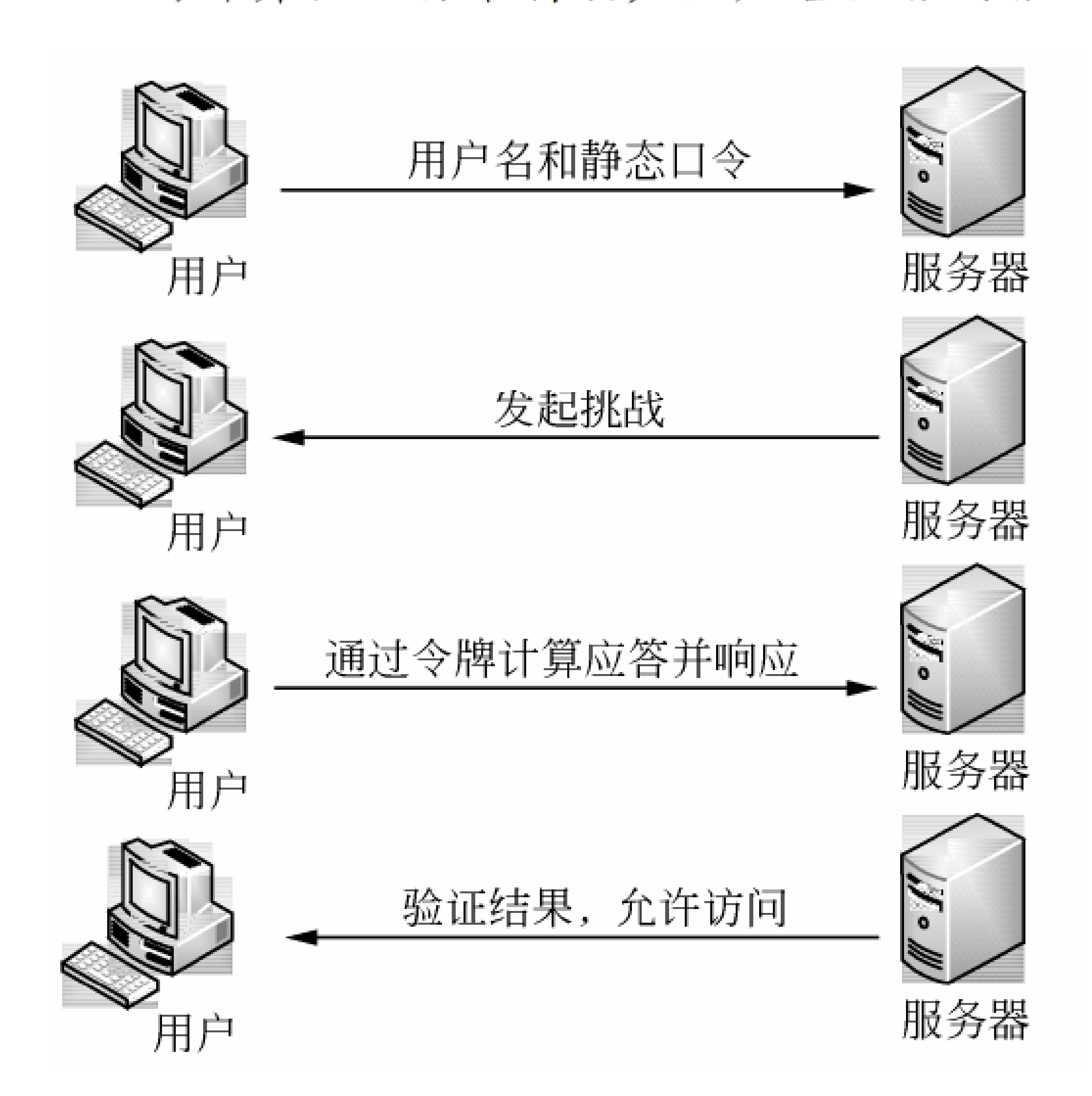


图 3-2　挑战应答认证过程

- **时间同步式**　在这种方式中，服务器上存储有用户的种子密钥，用来产生口令。用户拥有的口令卡里同样存储有用户的种子密钥。进行认证时，用户向系统提供 PIN 值以及由口令卡根据当前时间计算的口令值。服务器将用户提供的口令和自己计算所得的口令进行对比，认证用户。这样计算的口令值会随着时间的改变而改变，因此，实现了一次性口令认证。其存在的缺陷是必须保证服务器和认证卡中的时间严格同步，而由于网络在处理和传输数据时存着一定的延迟，往往会导致认证失败。在实际应用中，为了减少认证失败的次数，服务器常常

使用一个比口令卡大得多的持续时间作为有效的时间范围。当用户登录时，服务器会在有效的时间范围内产生很多个口令，如果其中有一个与用户的口令一致，就允许访问。这样做，虽然减少了认证失败的次数，但是却加大了服务器的运算负担，并且增加了第三方重复攻击的危险。

3.3.2 公钥认证

公钥认证要求每个用户首先产生一对由公钥和私钥组成的密钥对，并存储在文件中。每个密钥对由密钥产生装置产生，通常是 1024 到 2048 比特。用户把公钥公布出来，而私钥由本人保存。

公钥系统被认证系统用来增加系统的安全。中央认证服务器（通常称为访问控制服务器（ACS））负责使用公钥系统进行认证。当一个用户试图访问 ACS 时，ACS 查找用户的公钥，用它加密并向用户发送一个挑战。如果用户使用私钥对这个挑战的应答做了签名，那么这个用户就被认证为合法的。

公钥认证的实例主要包括安全套接层（SSL）认证、Kerberos 认证以及 MD5 认证。关于安全套接层（SSL）协议及 Kerberos 协议将在第 4 章作详细介绍，下面主要介绍 MD5 认证。

MD5 即 Message-Digest Algorithm 5（信息—摘要算法 5），在 20 世纪 90 年代初由 MIT Laboratory for Computer Science 和 RSA Data Security Inc 的 Ronald L. Rivest 开发出来，是计算机广泛使用的散列算法之一，其前身有 MD2、MD3 和 MD4。

MD5 是一个安全散列函数，它将任意长度的消息映射为一个 128 位的大整数，用以提供信息的完整性保护。对 MD5 算法简要的叙述可以为：MD5 以 512 位分组来处理输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出由 4 个 32 位分组组成，将这 4 个 32 位分组级联后将生成一个 128 位散列值。以下是每次操作中用到的 4 个非线性函数，其基本方式为求余、取余、调整长度、与链接变量进行循环运算，最终得出结果。

$$F(X, Y, Z) = (X \square Y) \square (\neg X \square Z)$$
$$G(X, Y, Z) = (X \square Z) \square (Y \square \neg Z)$$
$$H(X, Y, Z) = X \oplus Y \oplus Z$$
$$I(X, Y, Z) = Y \oplus (X \square \neg Z)$$

这 4 个函数的说明：如果 X、Y 和 Z 的对应位是独立和均匀的，那么结果的每一位也应该是独立和均匀的。F 是一个逐位运算的函数，即如果 X，那么 Y，否则 Z。函数 H 是逐位奇偶操作符。其中 ⊕、□、□、¬分别是抑或、与、或、非的符号。

图 3-3 简单描述了一个 MD5 运算的原理，它由类似的 64 次循环构成，分成 4 组 16 次。F 表示一个非线性函数；一个函数运算一次。M_i 表示一个 32 位的输入数据，K_i 表示一个 32 位常数，用来完成每次不同的计算。

MD5 的典型应用是对一段信息产生信息摘要，以防止被篡改。比如，在 UNIX/Linux 下有很多软件在下载的时候都会附带一个文件名相同，文件扩展名为.md5 的文件，在这个文件中通常只有一行文本，大致内容如下：

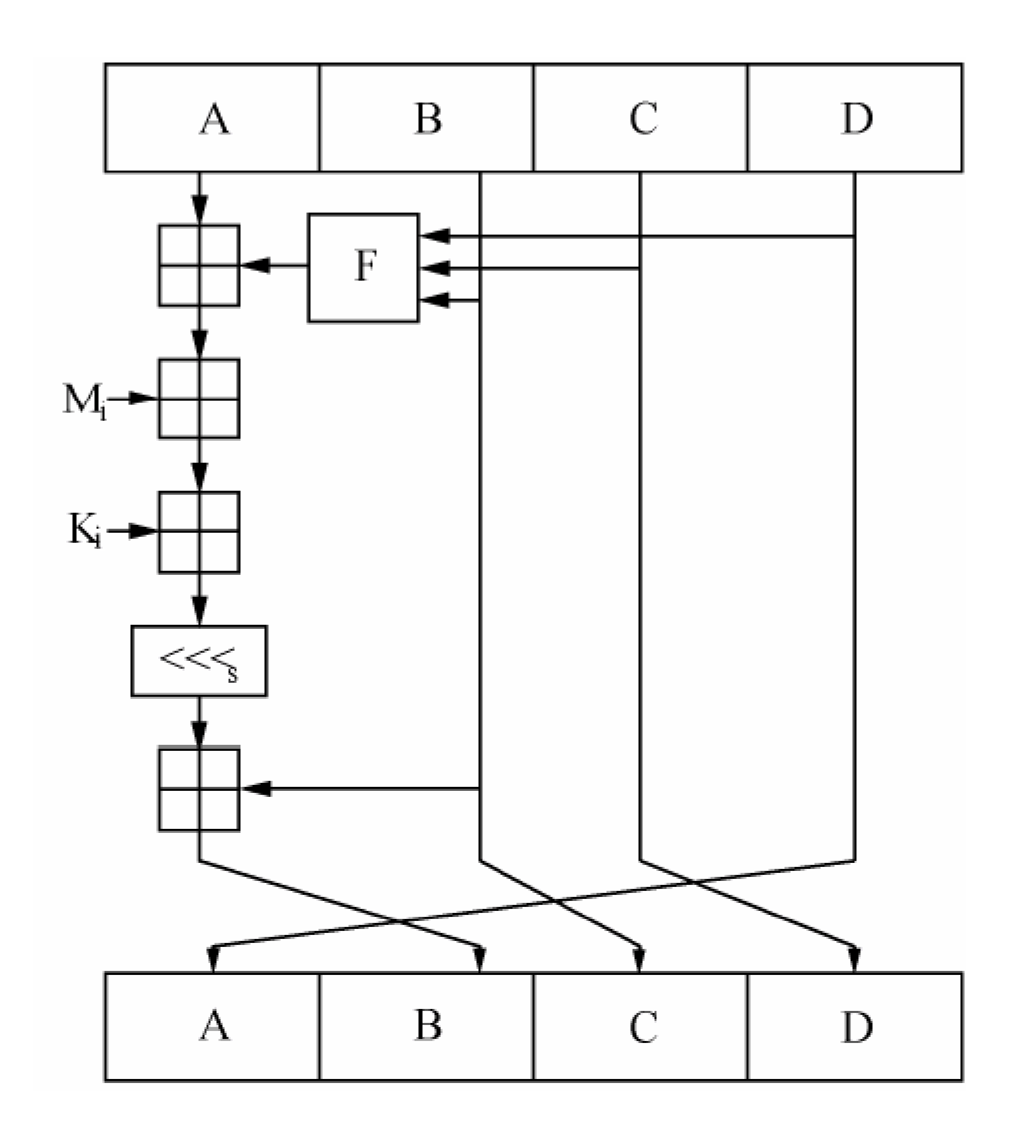


图 3-3　MD5 运算原理图

```
MD5 (testfile.tar.gz) = 0ha1as8gs0f726a831d895e2693387u6
```

这就是 testfile.tar.gz 文件的数字签名。MD5 将整个文件当作一个大文本信息，通过其不可逆的字符串变换算法，产生了该文件唯一的 MD5 信息摘要。如果在传播中，该文件的内容发生了任何形式的改变（如人为修改或者下载过程中的传输错误等），该文件的 MD5 值就会发生巨大变化，由此可以确定该文件是一个不正确的文件，而非提供者提供的那个文件。如果有一个第三方的认证机构，用 MD5 还可以防止文件作者的“抵赖”，这就是所谓的数字签名应用。

MD5 还可以用来进行认证。事实上，MD5 认证过程非常简单。如在 UNIX 系统中用户的口令是以 MD5 经 Hash 运算后存储在文件系统中。当用户登录时，系统把用户输入的口令进行 MD5 Hash 运算，然后将其与保存在文件系统中的 MD5 值进行比较，进而确定输入的口令是否正确。通过这样的步骤，系统在并不知道用户口令明文的情况下就可以确定用户登录系统的合法性，可以避免用户的口令被具有系统管理员权限的用户知道。

3.3.3　远程认证

远程认证用来认证从远程主机拨号接入访问控制服务器 ACS 的用户。有多种远程认证的方法，包括使用安全的远程过程调用（RPC）、Dail-in 拨号认证以及 RADIUS 认证。

1．安全 RPC 认证

在很多服务中，尤其是 Internet 服务，客户端并不想向服务器认证自己的身份，服务器也不要求对所有的客户端进行认证。这种类型的服务，例如网络文件系统（NFS），比起其他的服务要求更强的安全性。RPC 认证子系统的数据包是开放式的，因此 RPC 可以使用不同格式和多种类型的认证，包括 NULL 认证、UNIX 认证、DES 认证、DES 认证协议、Diffie-Hellman 加密。

无论 RPC 使用哪种类型的加密算法，对于服务器和用户之间的密钥调用，提供拨号

服务的服务器都要求对用户进行认证。

2. Dial-in 拨号认证

用户进行远程呼叫时，拨号入网过程中经常被要求输入口令。在拨号入网连接中，点对点形式是最普遍的一种方式。用户成功登录之前必须要进行认证。有很多种拨号认证协议，例如，PPP 认证机制包括的口令认证协议（PAP）、挑战握手协议（CHAP）以及扩展认证协议（EAP）。

3. 远程用户拨号认证（RADIUS）

RADIUS 协议最初是由 Livingston 公司提出的，最初的目的是为拨号用户进行认证和计费。多次修改后形成了一项通用的认证计费协议。

RADIUS 是一种 C/S 结构的协议，其客户端最初是 NAS（Net Access Server）服务器，现在任何运行 RADIUS 客户端软件的计算机都可以成为 RADIUS 的客户端。RADIUS 协议认证机制灵活，可以采用 PAP、 CHAP 或 UNIX 登录认证等多种方式。

用户接入 NAS，NAS 向 RADIUS 服务器使用 Access-Require 数据包提交用户信息，包括用户名、口令等相关信息，其中用户口令是经过 MD5 加密的，双方使用共享密钥，这个密钥不经过网络传播；RADIUS 服务器对用户名和口令的合法性进行检验，必要时可以提出一个 Challenge，要求进一步对用户认证，也可以对 NAS 进行类似的认证；如果合法，给 NAS 返回 Access-Accept 数据包，允许用户进行下一步工作，否则返回 Access-Reject 数据包，拒绝用户访问；如果允许访问，NAS 向 RADIUS 服务器提出计费请求 Account- Require，RADIUS 服务器响应 Account-Accept，对用户的计费开始，同时用户可以进行自己的相关操作。

3.3.4 匿名认证

在对用户进行认证的时候往往需要用户出示某些个人信息对其身份进行认证，但是并非所有用户都愿意这样做。能不能在不确认对方具体身份的前提下就能鉴别对方，而给与对方某种相应的权利呢？比如很多商场都有贵宾卡制度，顾客可以在购物的时候出示贵宾卡从而享受一定的打折优惠。在结账的时候，收银员并不知道顾客的真实身份，只是根据顾客所出示的贵宾卡就承认顾客所要求的打折权利。这个例子的特点是认证机构（收银员）在信任对方并赋予对方权利的时候并不知道对方的具体身份。匿名认证技术正是来源这样一种要求，被认证者要求某种权利，而同时不提供具体的个体信息。

匿名认证，从原理上可以简单地归结为将认证过程和个人信息相分离。按照分离的手段不同，匿名认证可以有多种实现方式。

3.3.5 基于数字签名的认证

基于数字签名的认证是另一种不需要口令和用户名的认证技术。数字签名是被信息接收者或任何第三方用来验证发送者身份以及信息的一种密码方案。这种方案可能包含

一系列的算法和函数，例如数字签名算法（DSA）、椭圆曲线数字签名算法（ECDSA）、账户认证数字签名、认证函数以及签名函数等。

数字签名和手写签名的作用是一样的，也是来认证签名者。数字签名被用来认证签名者已经答应的事情，防止他收回自己的承诺。像纸质签名一样，数字签名在信息和信息签名者之间建立了一种法律的和心理的联系。

数字签名使用了 PKI，所以使用该方案就必须获得一个公钥和一个私钥。私钥被用户保存，用来对文件进行签名。文件认证者使用签名者的公钥来确认签名者就是他所声明的那个人。用户向 ACS 发送认证请求和密钥。接到认证请求之后，服务器使用它的私钥来解密这个请求。之后，使用签名者的公钥就可以验证签名了。

习　题

一、选择题

1. 下面哪项不属于口令认证？（　　）
   A. 可重用口令认证
   B. 一次性口令认证
   C. 安全套接层认证
   D. 挑战应答口令认证
2. 公钥认证不包括下列哪一项？（　　）
   A. SSL 认证
   B. Kerberos 认证
   C. 安全 RPC 认证
   D. MD5 认证

二、问答题

1. 简述认证的组成及其功能。
2. 简述 S/Key 口令认证原理。
3. Kerberos 是如何认证的？

课后实践

802.1X 认证完整配置过程说明

802.1x 协议起源于 802.11 协议，后者是 IEEE 的无线局域网协议，制定 802.1x 协议的初衷是为了解决无线局域网用户的接入认证问题。IEEE802LAN 协议定义的局域网并不提供接入认证，只要用户能接入局域网控制设备（如 LANS witch）就可以访问局域网中的设备或资源。这在早期企业网有线 LAN 应用环境下并不存在明显的安全隐患。但是随着移动办公及驻地网运营等应用的大规模发展，服务提供者需要对用户的接入进行控制和配置。尤其是 WLAN 的应用和 LAN 接入在电信网上大规模开展，有必要对端口加以控制以实现用户级的接入控制，802.lx 就是 IEEE 为了解决基于端口的接入控制(Port-Based Network Access Contro1) 而定义的一个标准。

802.1x 协议认证过程如下。

（1）客户端向接入设备发送一个 EAPoL-Start 报文，开始 802.1x 认证接入。

（2）接入设备向客户端发送 EAP-Request/Identity 报文，要求客户端将用户名送上来。

（3）客户端回应一个 EAP-Response/Identity 给接入设备的请求，其中包括用户名。

（4）接入设备将 EAP-Response/Identity 报文封装到 RADIUS Access-Request 报文中，发送给认证服务器。

（5）认证服务器产生一个 Challenge，通过接入设备将 RADIUS Access-Challenge 报

文发送给客户端，其中包含有 EAP-Request/MD5-Challenge。

（6）接入设备通过 EAP-Request/MD5-Challenge 发送给客户端，要求客户端进行认证。

（7）客户端收到 EAP-Request/MD5-Challenge 报文后，将密码和 Challenge 做 MD5 算法后的 Challenged-Pass-word，在 EAP-Response/MD5-Challenge 回应给接入设备。

（8）接入设备将 Challenge，Challenged Password 和用户名一起送到 RADIUS 服务器，由 RADIUS 服务器进行认证。

（9）RADIUS 服务器根据用户信息做 MD5 算法，判断用户是否合法，然后回应认证成功/失败报文到接入设备。如果成功，携带协商参数，以及用户的相关业务属性给用户授权；如果认证失败，则流程到此结束。

（10）如果认证通过，用户通过标准的 DHCP 协议（可以是 DHCP Relay），通过接入设备获取规划的 IP 地址。

（11）如果认证通过，接入设备发起计费开始请求给 RADIUS 用户认证服务器。

（12）RADIUS 用户认证服务器回应计费开始请求报文。用户上线完毕。

802.1x 认证的网络拓扑结构如图 3-4 所示。

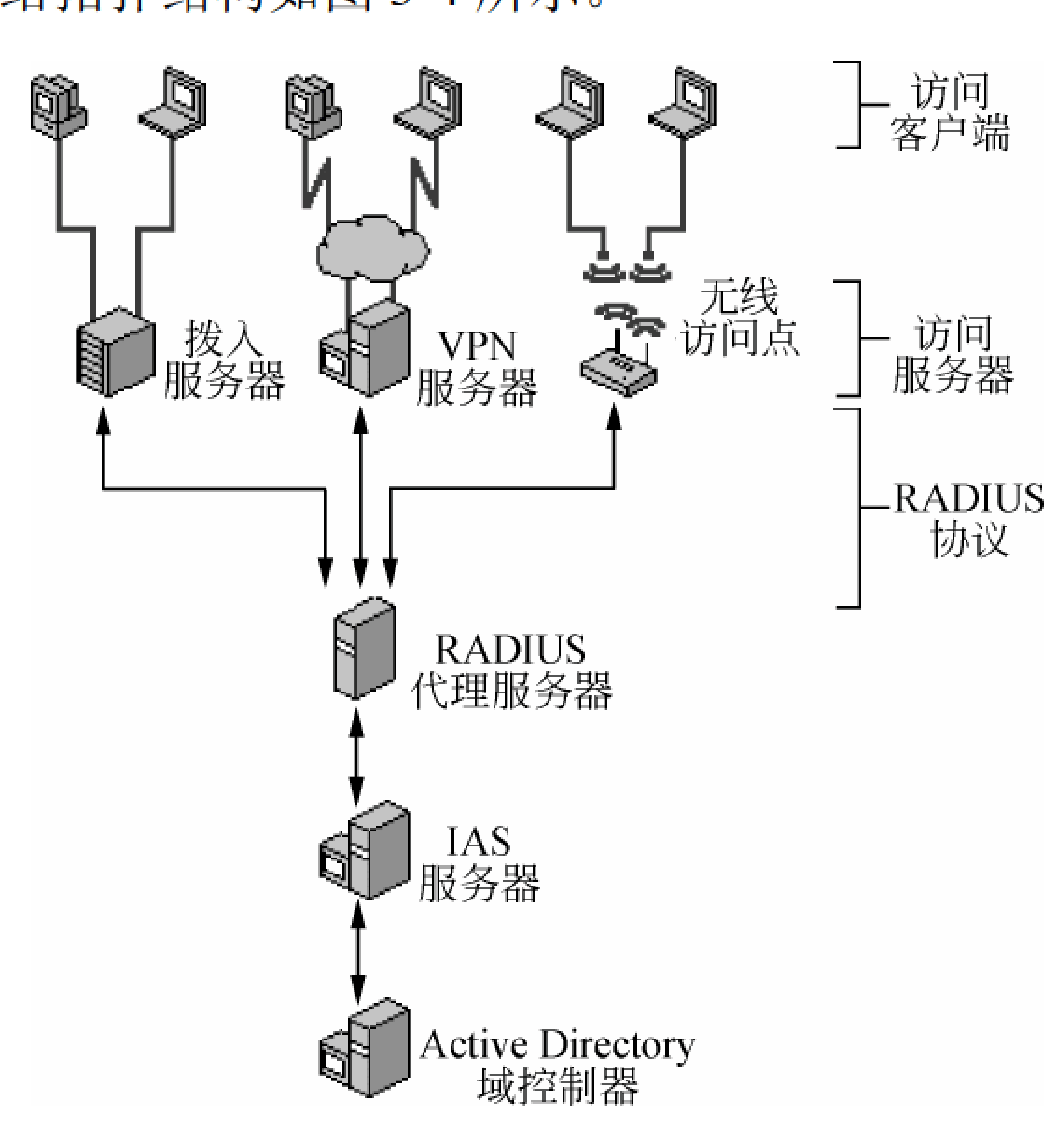


图 3-4　802.1x 认证的网络拓扑结构

认证客户端采用无线客户端，无线接入点是用 Cisco2100 Wireless Controller，服务器安装 Windows Server 2003 sp1；所以完整的配置方案应该对这三者都进行相关配置，思路是首先配置 RADIUS Server 端，其次是配置无线接入点，最后配置无线客户端，这三者的配置先后顺序是无所谓的。

配置内容见表 3-1。

表 3-1　配置方案

配置	RADIUS Server	Access Pointer	Wireless Client
IP Address	192.168.1.188	192.168.1.201	DHCP 自动获得
Operate System	Windows Server 2003	CISCO Wireless controller	Windows XP

1. 配置 RADIUS Server 步骤

配置 RADIUS Server 的前提是要在服务器上安装 Active Directory、IAS（internet 验证服务）、IIS 管理器（Internet 信息服务管理器）和证书颁发机构。

如果没有安装 AD，在“开始”→“运行”→“命令”文本框中输入命令“dcpromo”，然后按照提示安装就可以了。

如果没有安装证书颁发机构，就在“控制面板”→“添加删除程序”→“添加/删除 Windows 组件”→“Windows 组件向导”的组件中选择“证书服务”并按提示安装。

如果没有安装 IAS 和 IIS，就在“控制面板”→“添加删除程序”→“添加/删除 Windows 组件”→“Windows 组件向导”的组件中选择“网络服务”，按提示完成安装。

在 AD 和证书服务没有安装时，要先安装 AD 然后安装证书服务，如果此顺序反了，证书服务中的企业根证书服务则不能选择安装。

在这 4 个管理部件都安装的条件下，可以配置 RADIUS 服务器了。

2. 默认域安全设置

单击“开始”→“管理工具”→“域安全策略”命令，进入默认域安全设置，展开“安全设置”→“账户策略”→“密码策略”，结果如图 3-5 所示。在右侧列出的策略中，右击“密码必须符合复杂性要求”并选择“属性”命令，将这个策略设置成“已禁用”，如图 3-6 所示。

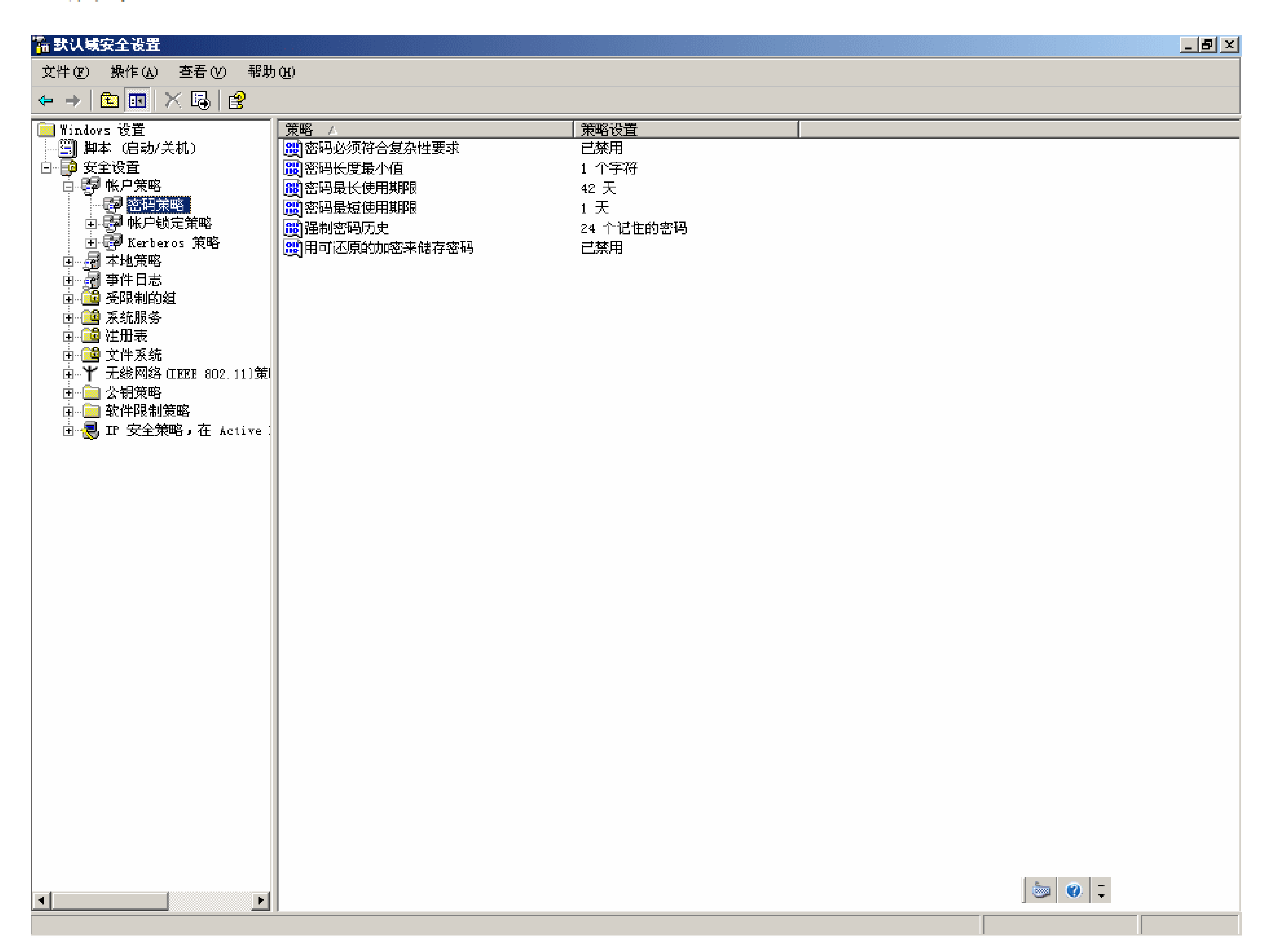


图 3-5　密码策略

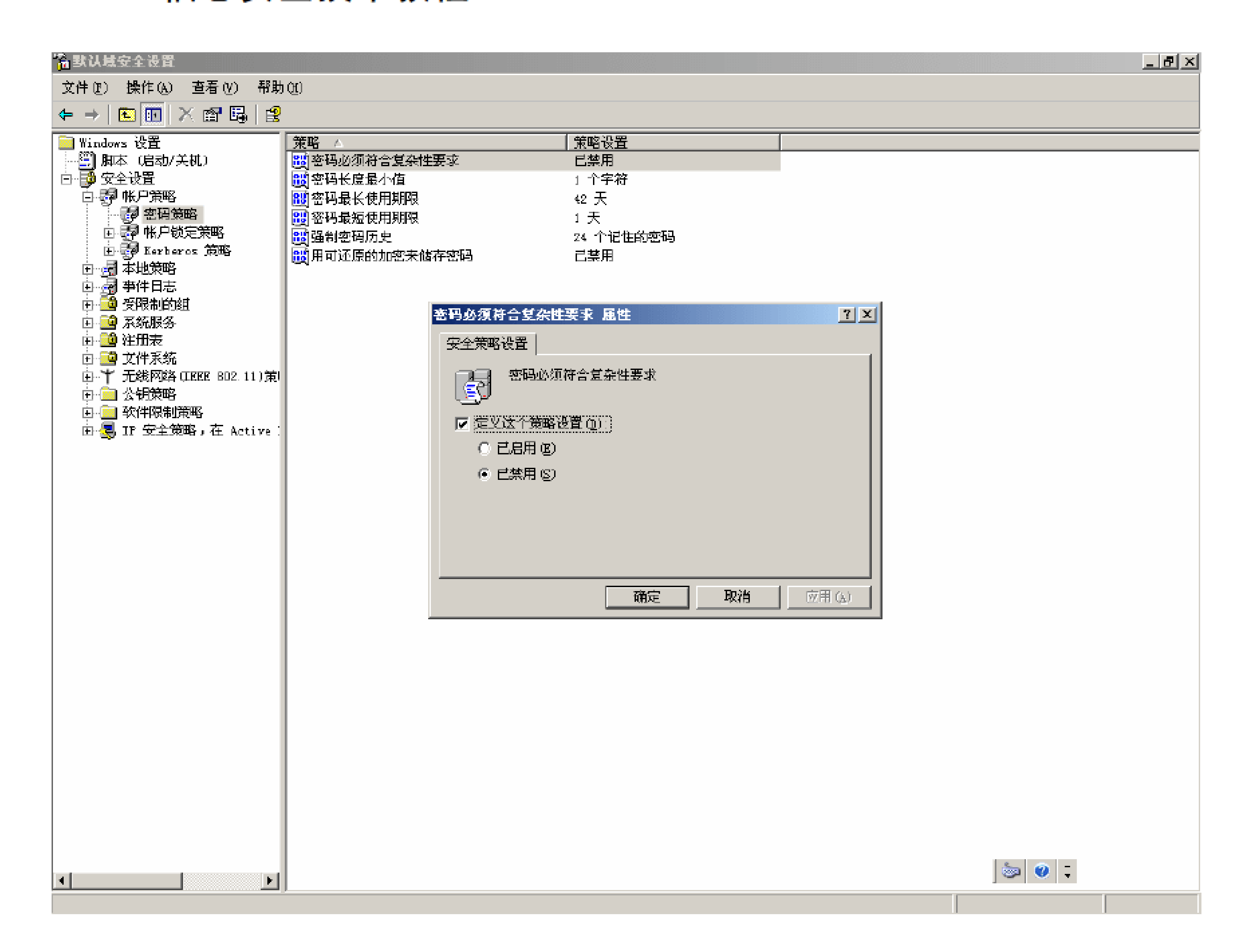


图 3-6 安全策略设置

在完成此设置后，后面创建客户端密码时会省去一些麻烦。

3．配置 Active Directory 用户和计算机

单击“开始”→“管理工具”→Active Directory 命令，展开根域 zhanggc.com（根域的命名方式见帮助），在 Users 中新建一个组，如图 3-7 所示。

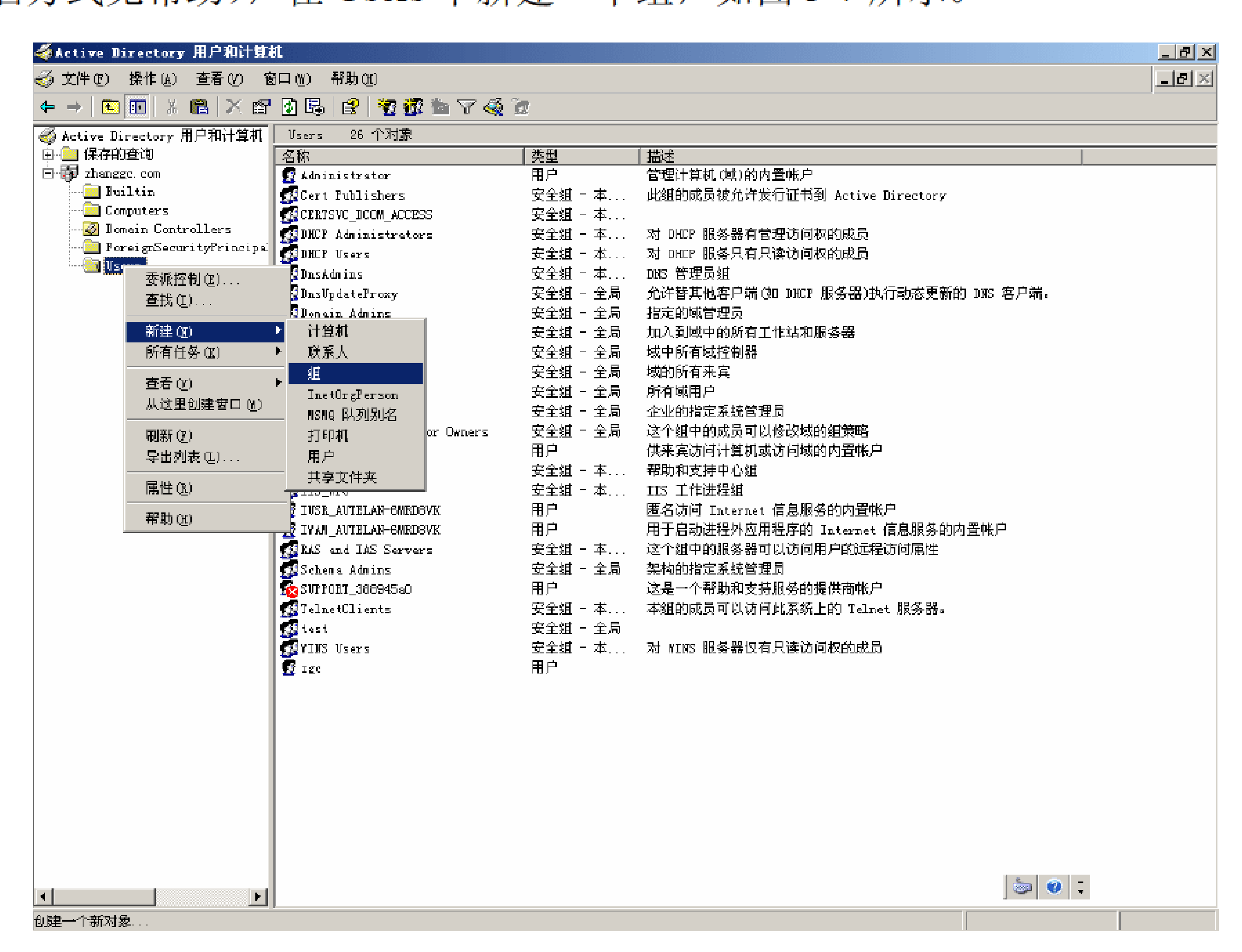


图 3-7 新建组

将新建的组归类到安全组，作用于全局，如图 3-8 所示，单击“确定”按钮即完成新建组。



图 3-8　新建组设置

再在 Users 中新建一个用户，如图 3-9 所示。这个用户的姓名一定要记住，它是在无线客户端证书验证时要用的名字。

新建对象 － 用户
创建在： zhanggc.com/Users
姓(L)： z
名(F)： gongchang　英文缩写(I)：
姓名(A)： zgongchang
用户登录名(U)：
zhanggongchang　@zhanggc.com
用户登录名(Windows 2000 以前版本)(W)：
ZHANGGC\　zhanggongchang
< 上一步(B)　下一步(N) >　取消

图 3-9　新建用户

单击“下一步”按钮，输入密码，这个密码一定要记住，它是在无线客户端要用的密码，单击“下一步”按钮完成新创建用户。

将新建用户 zgongchang 加入到新建的组 test1 中，如图 3-10 所示。

选择组时，单击“高级”按钮后再单击“立即查找”按钮，选择想加入的组，如图 3-11 所示。以后两次单击“确定”按钮即可，结果如图 3-12 所示。

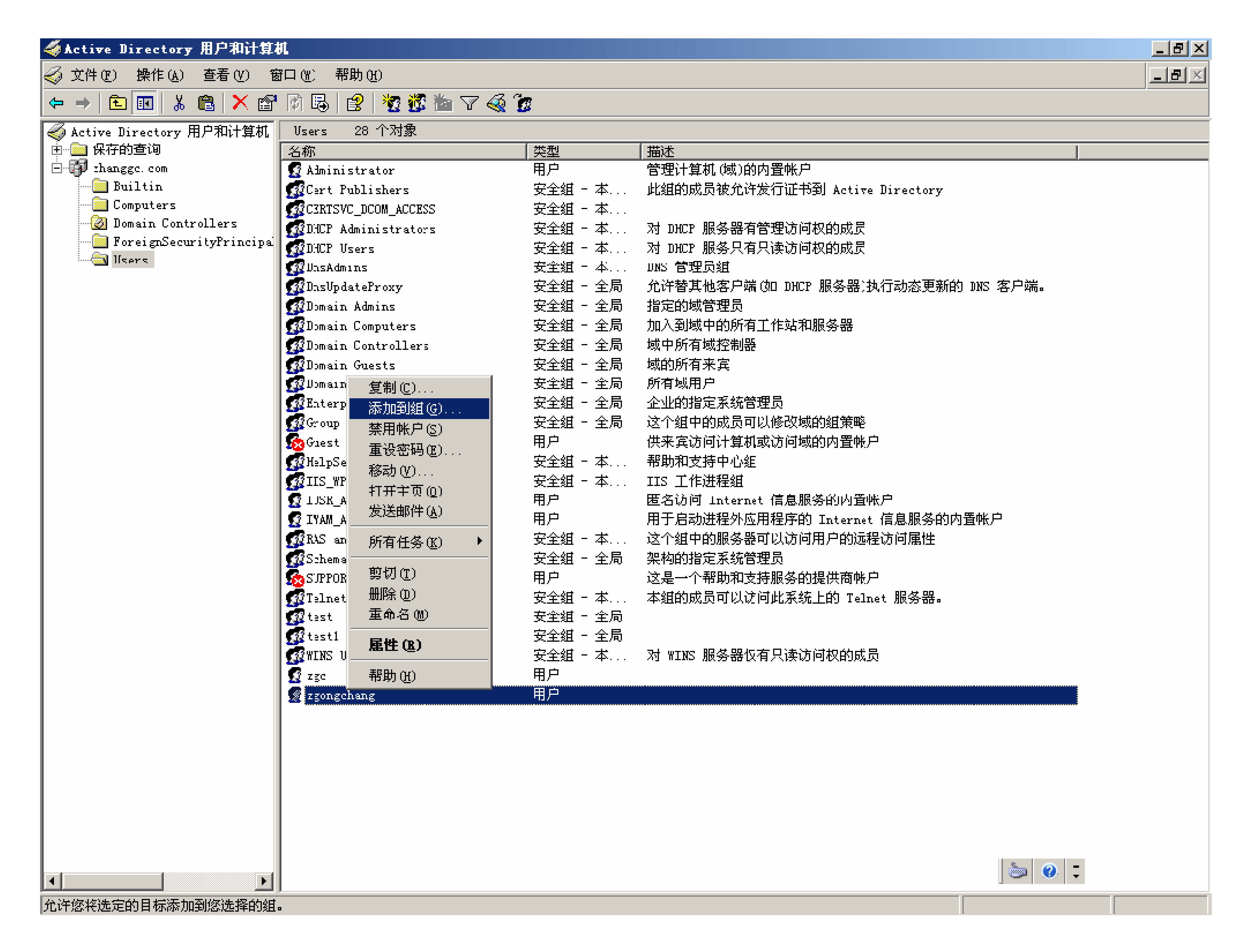


图 3-10　用户添加到组

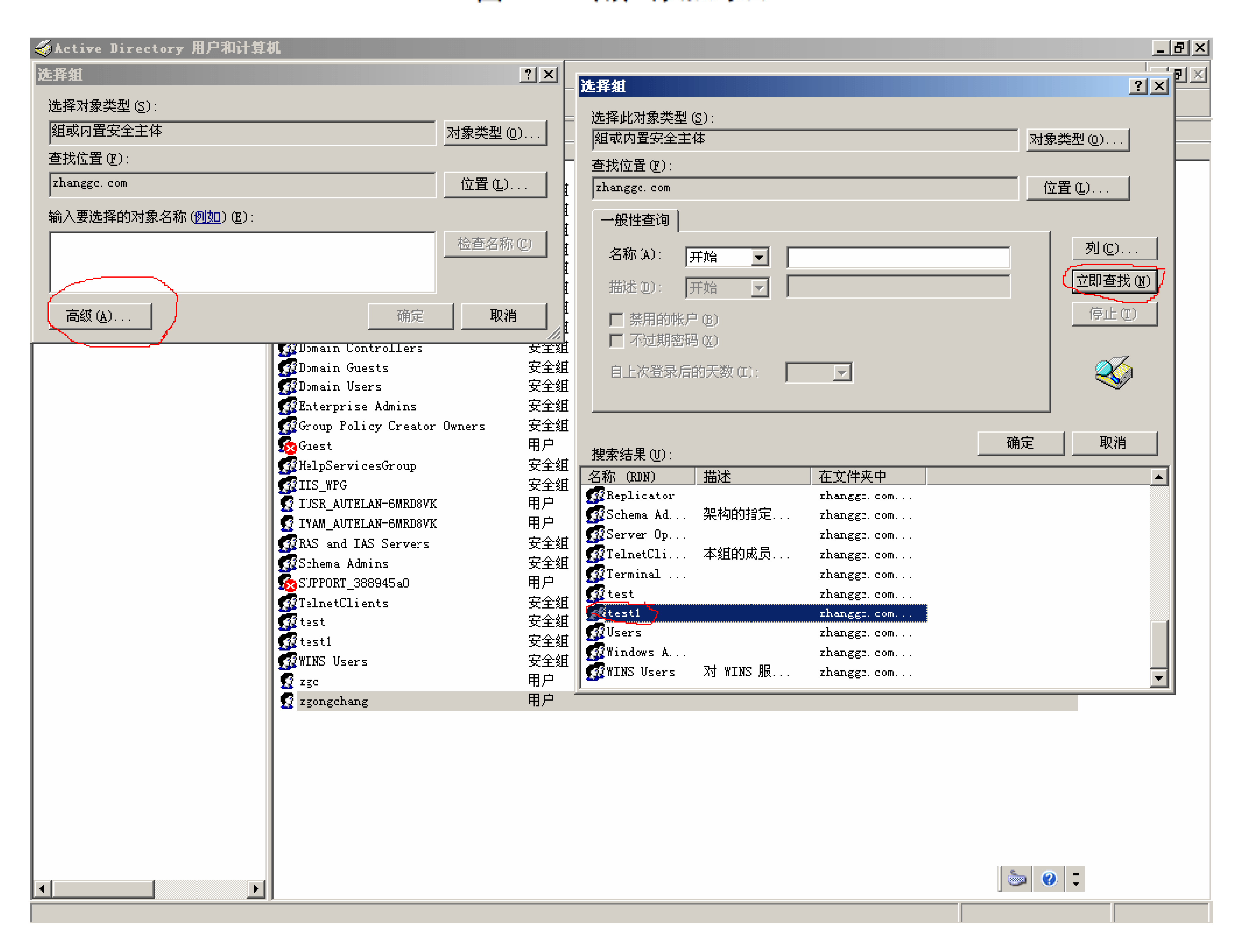


图 3-11　选择组

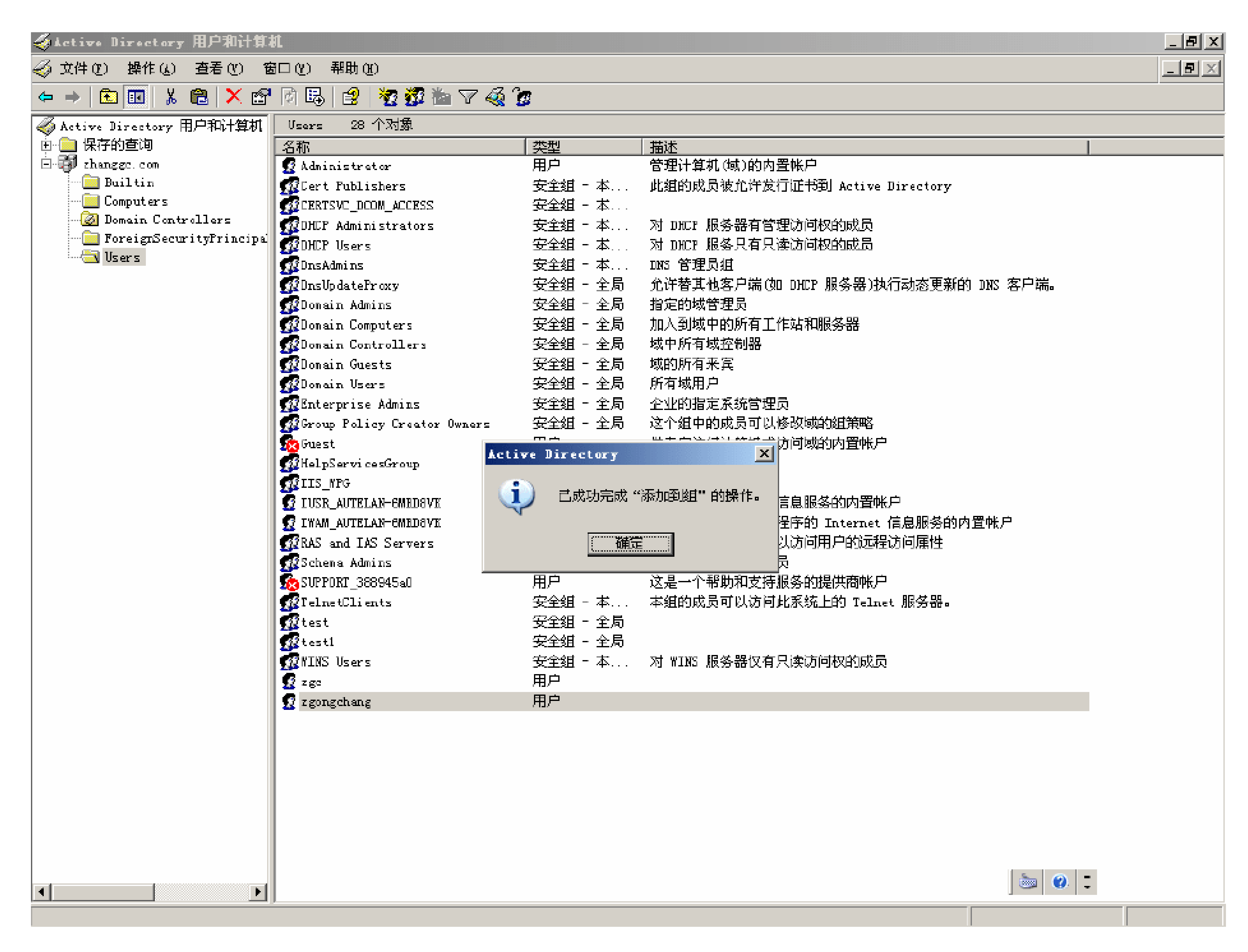


图 3-12　成功添加到组

右击新建组 test1，选择“属性”命令，开始配置新建的组（新建用户 zgongchang 也在其中），选择“隶属于”选项卡，单击“添加”按钮，如图 3-13 所示，在选择组中单击“高级”按钮。

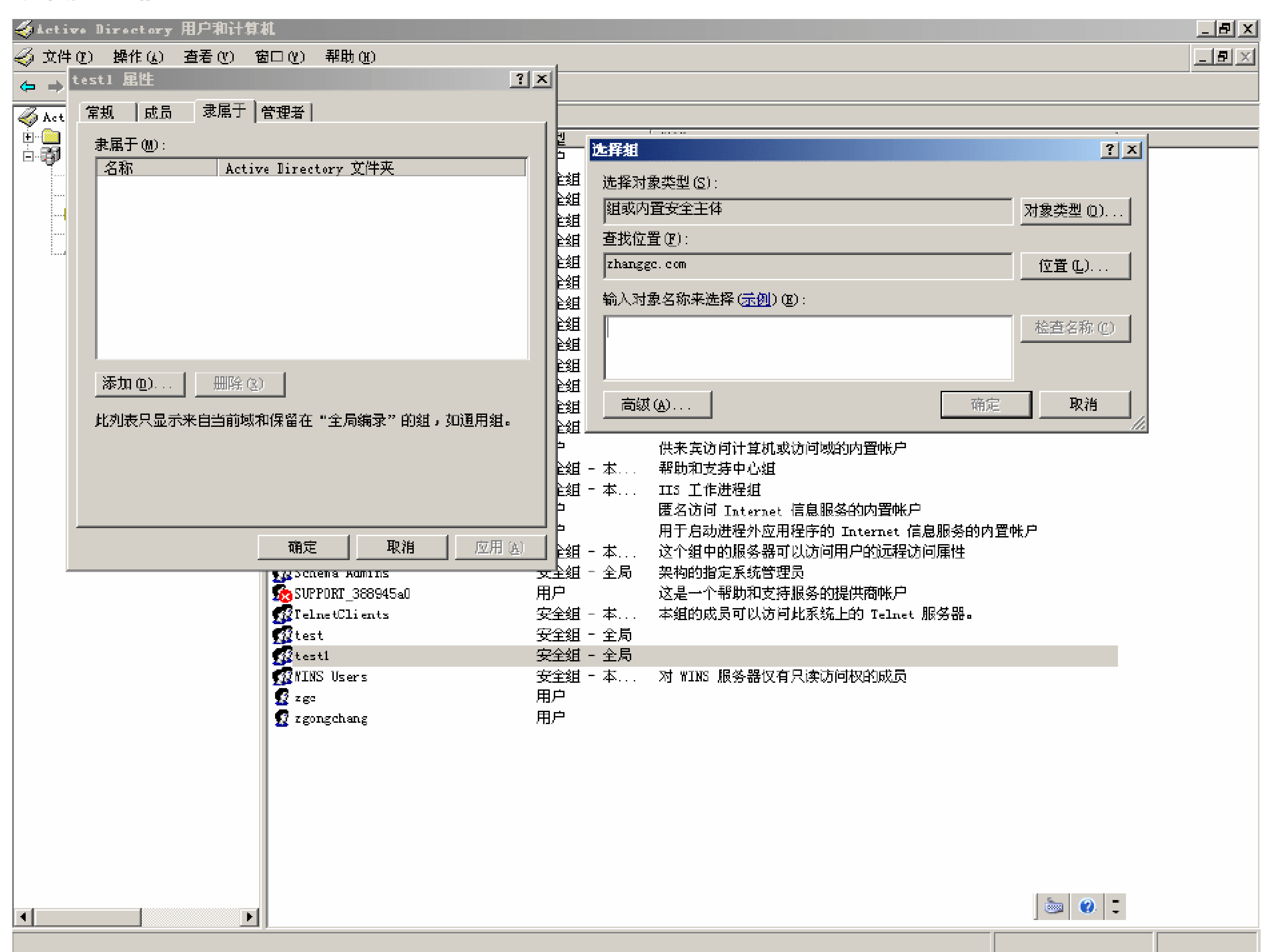


图 3-13　新建组属性

单击“立即查找”按钮，选择所有组（在保险情况下，最好全选），如图 3-14 所示，然后依次单击“确定”按钮，“隶属于”设置完毕。

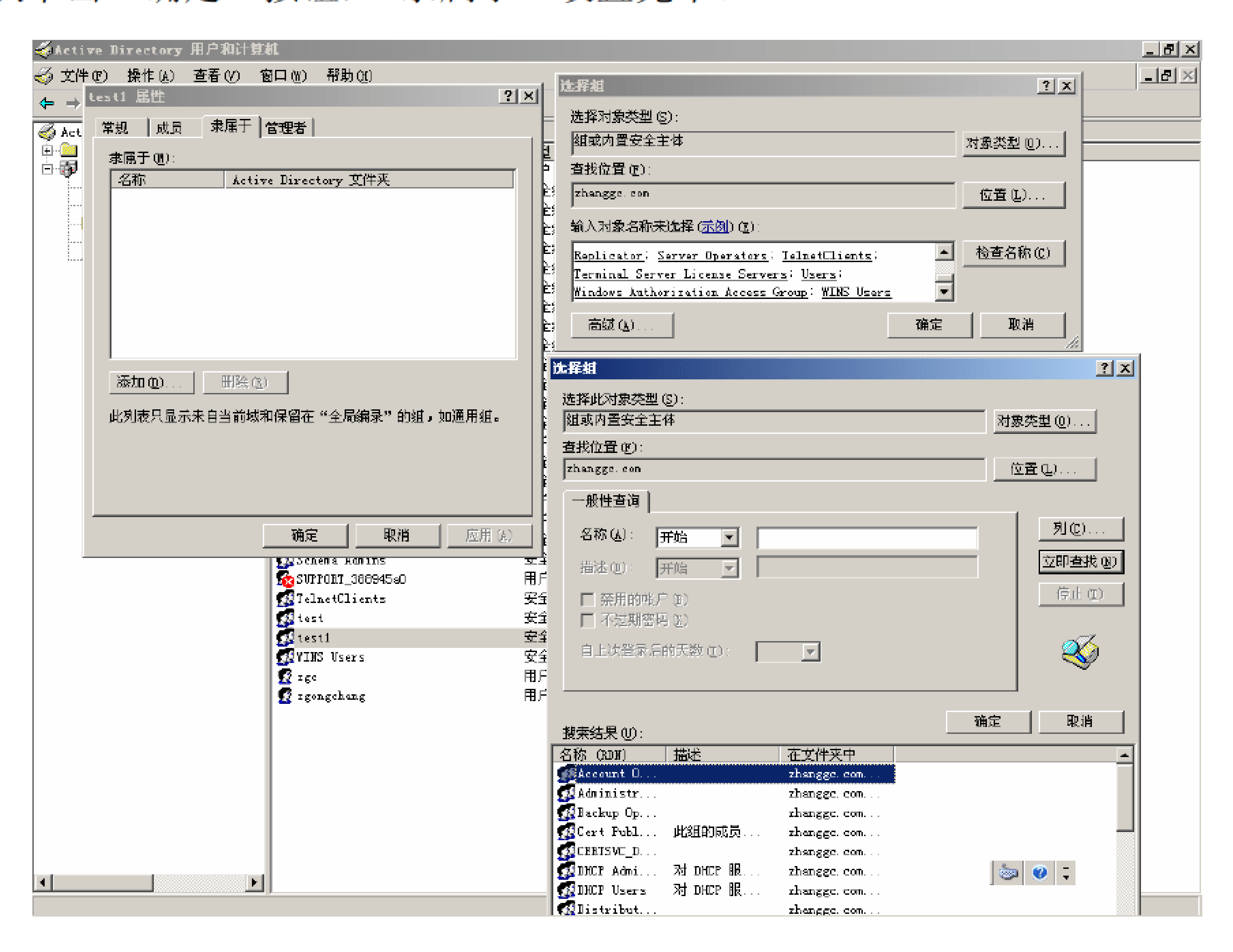


图 3-14　选择组

选择“管理者”选项卡，和上面相似，选择被“zgongchang”管理，如图 3-15 和图 3-16 所示。

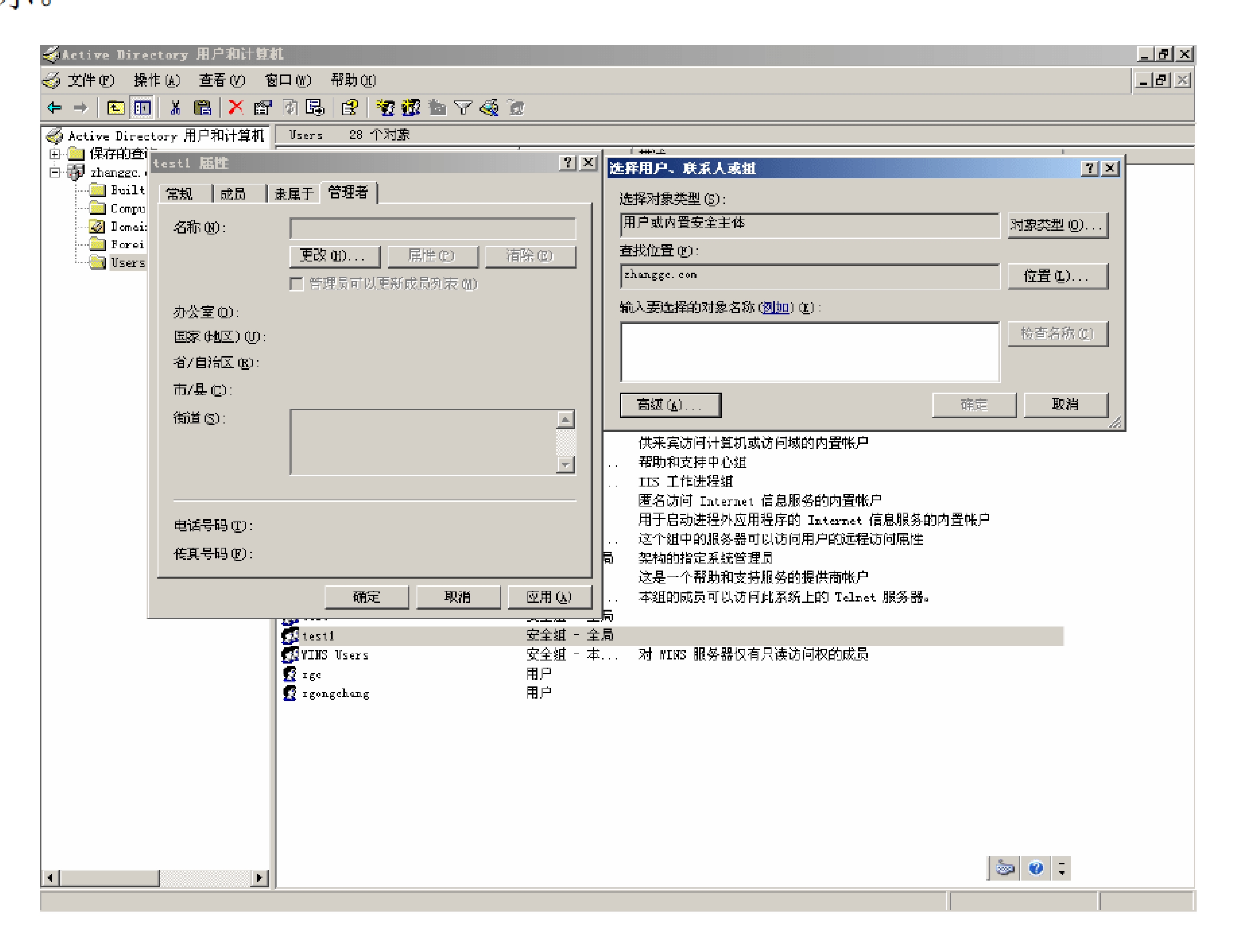


图 3-15　管理者设置 1

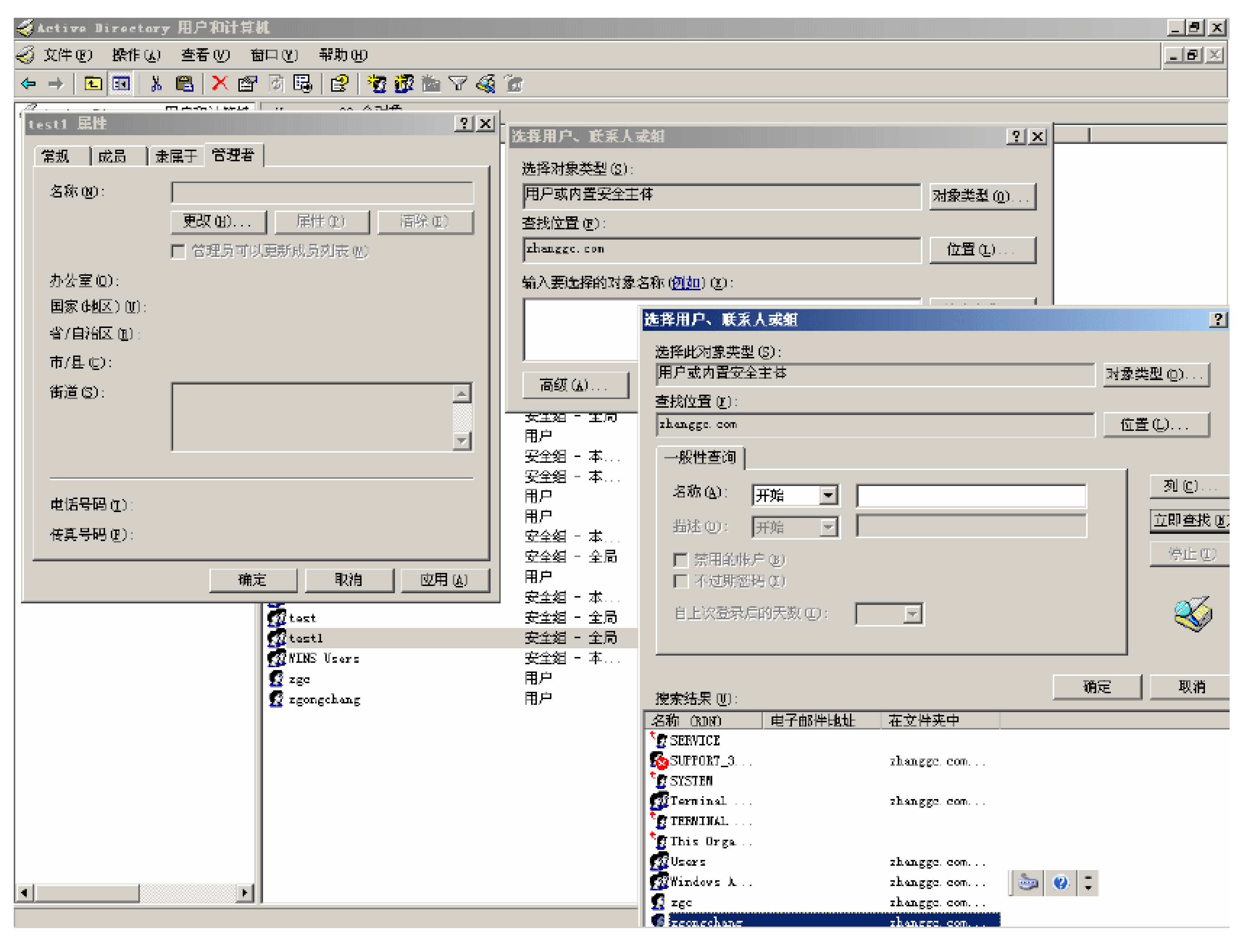


图 3-16　管理者设置 2

至此，AD 配置完成。

4．设置自动申请证书

下面是说明如何使用组策略管理单元，在默认组策略对象中创建自动申请证书。

单击“开始”→“管理工具”→“Active Directory 用户和计算机”命令，会显示在根域下的各个单元，右击根域（zhanggc.com），选择“属性”命令，如图 3-17 所示。

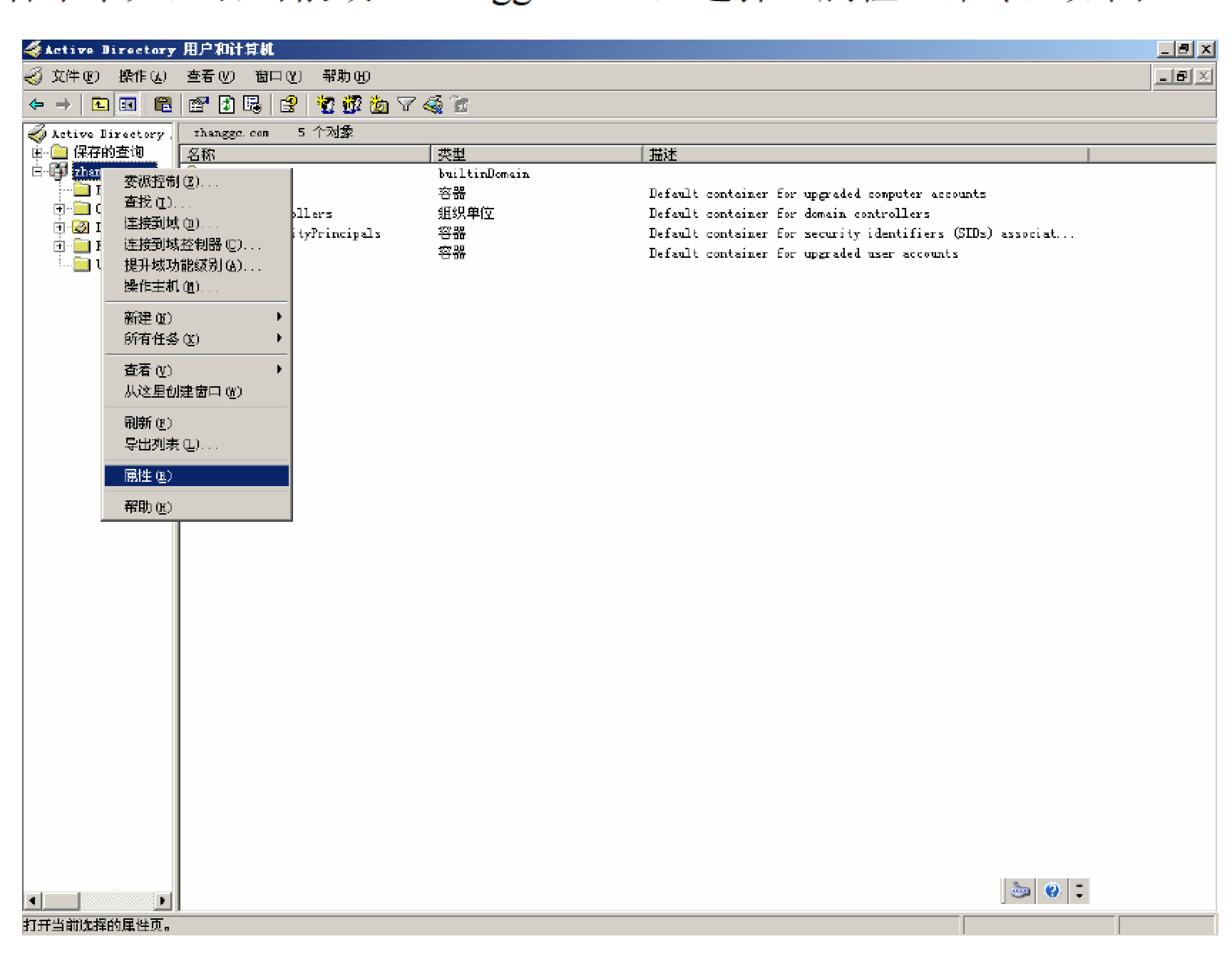


图 3-17　右击根目录

打开根域属性的配置框，选择“组策略”选项卡，如图 3-18 所示，选中 Default Domain Policy 项，并单击“编辑”按钮，就会进入“组策略编辑器”，展开“计算机配置”→“Windows 设置”→“安全设置”→“公钥策略”→“自动申请证书”，右击，选择“新建”→“自动证书申请”命令，如图 3-19 所示，下面会进入自动证书申请向导中，如图 3-20 所示，“证书模版”一般选用“计算机”，如图 3-21 所示，单击“下一步”按钮即可完成自动申请证书，结果如图 3-22 所示。

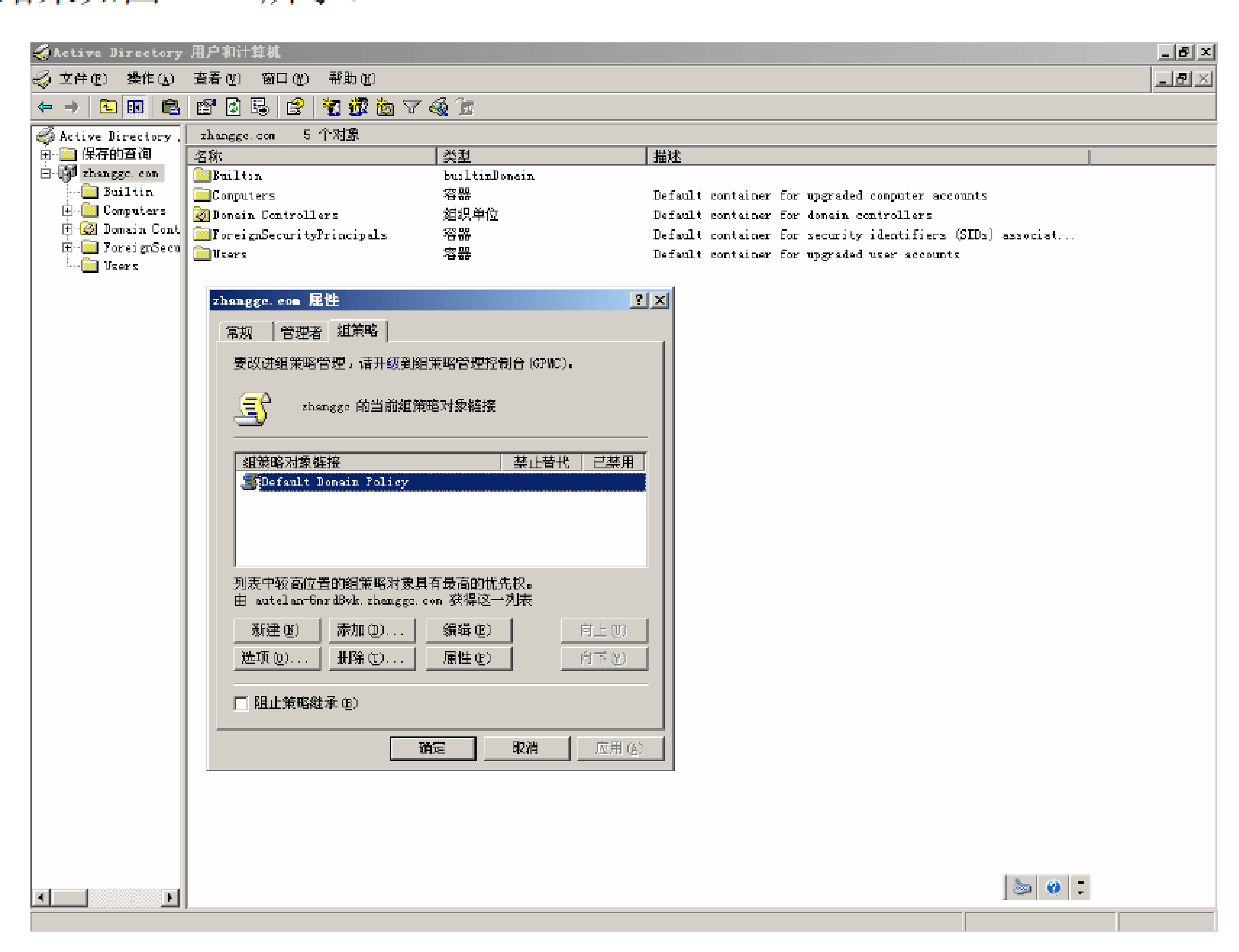


图 3-18 组策略

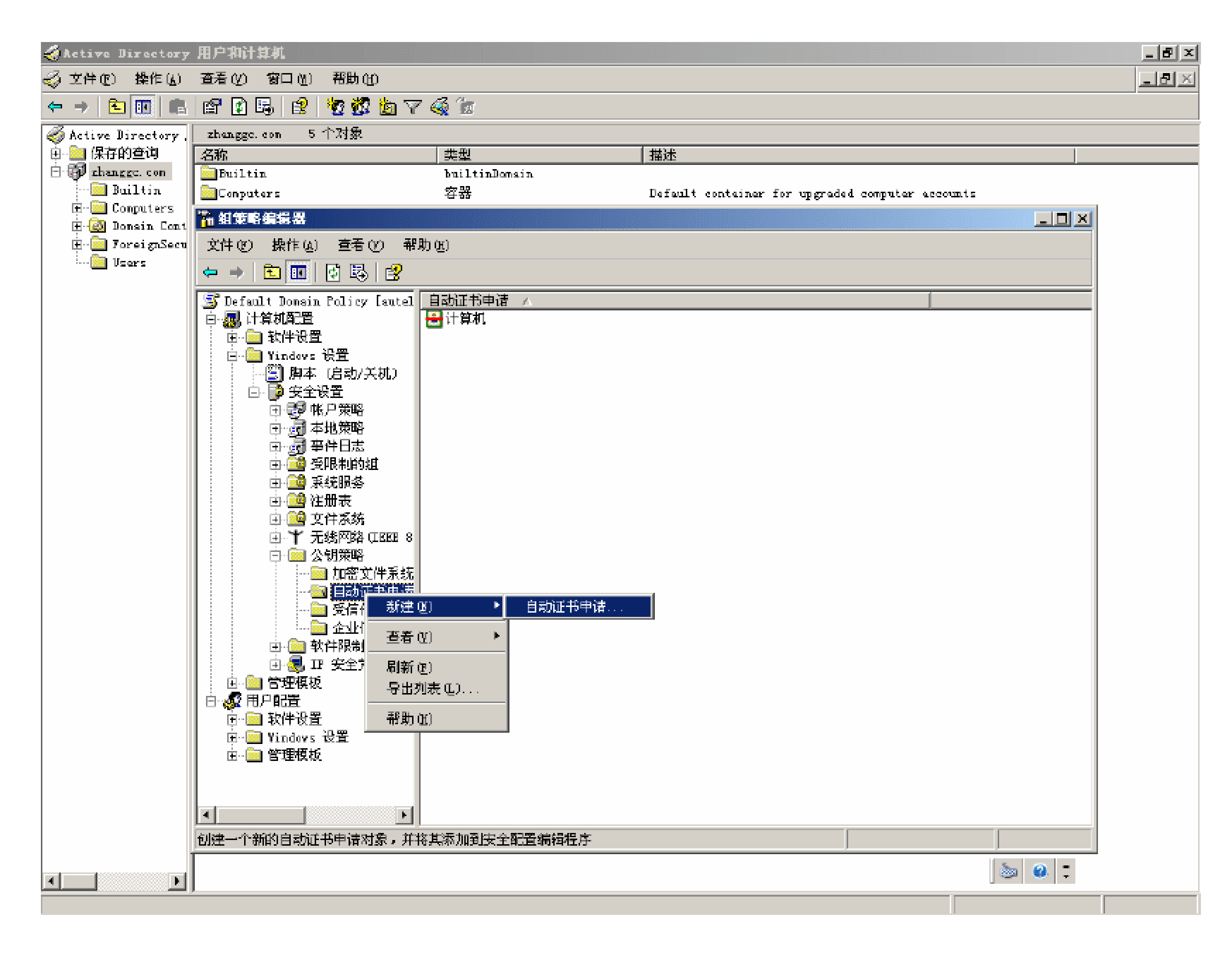


图 3-19 新建自动证书申请

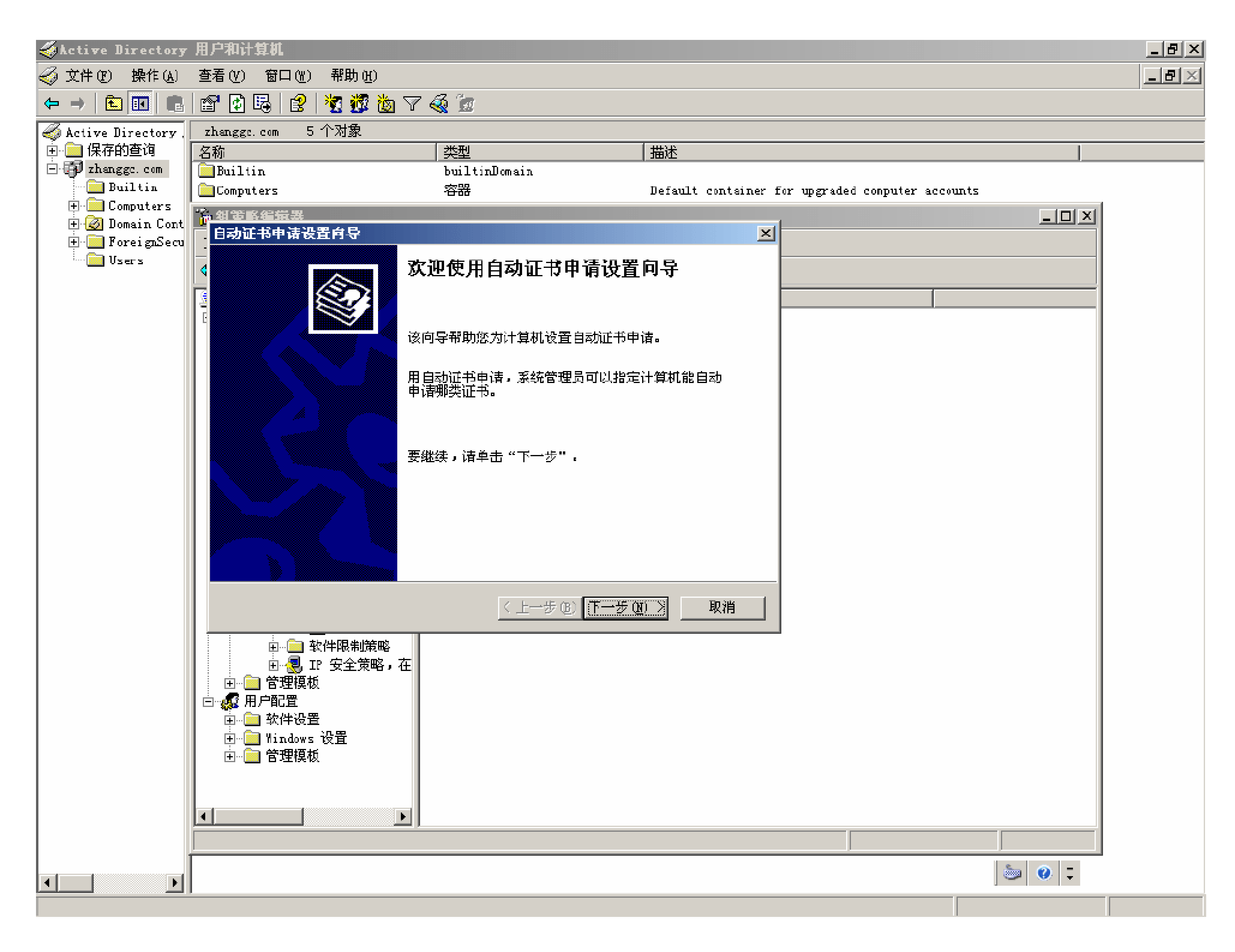


图 3-20　自动证书申请设置

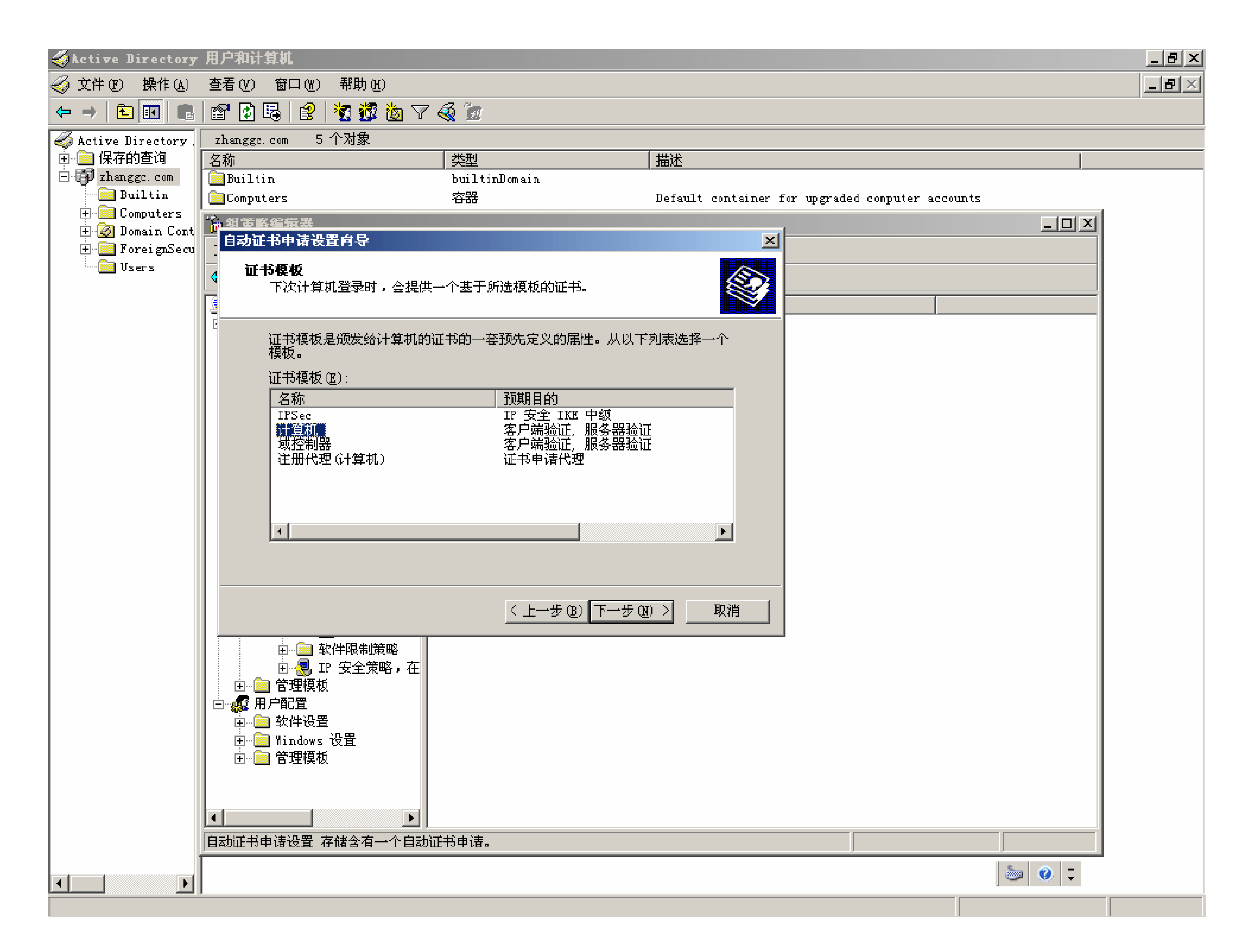


图 3-21　证书模板选择

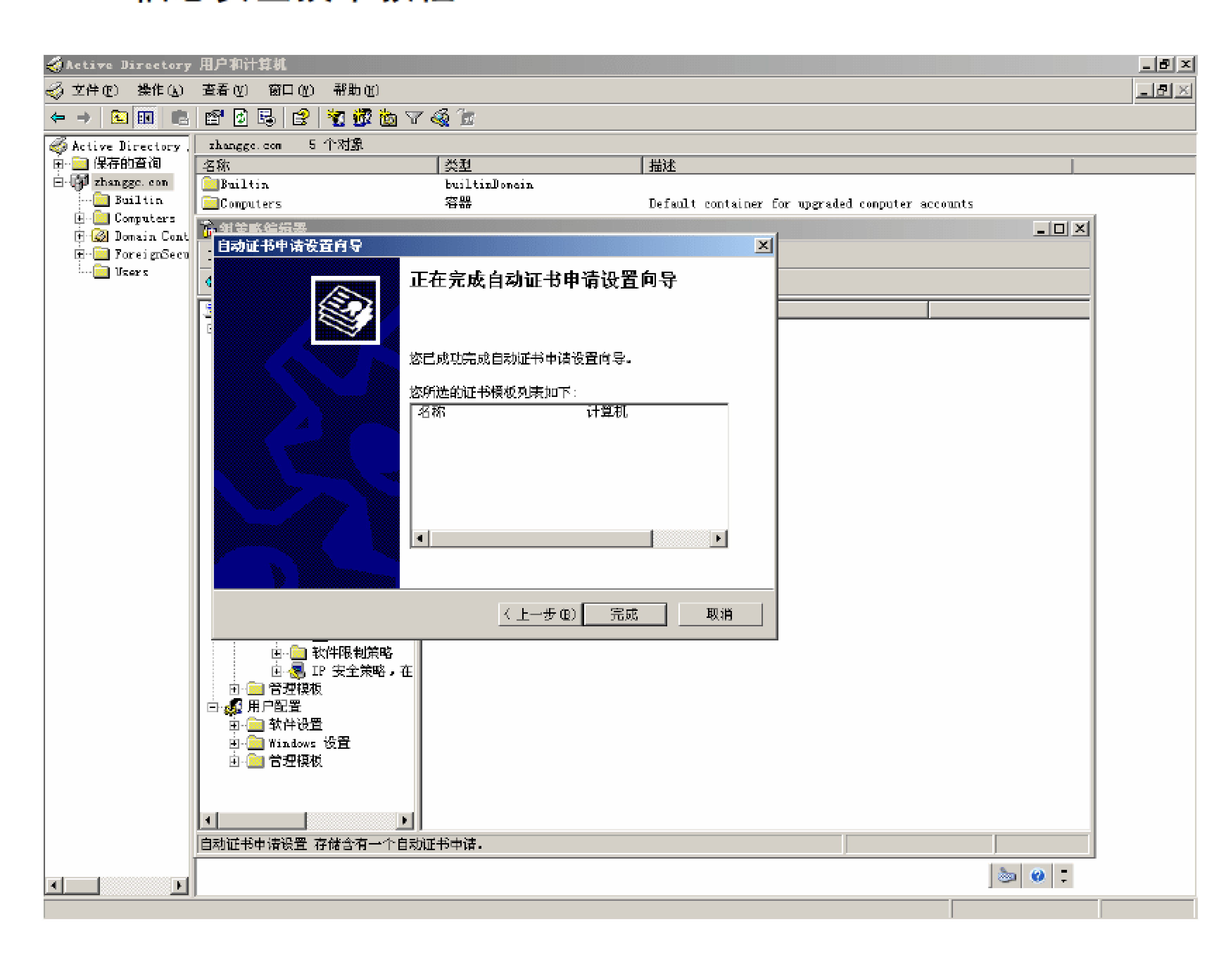


图 3-22　完成自动证书申请设置

自动申请证书以后，在“组策略编辑器”的“自动申请证书”右侧框中会有一个申请成功的“计算机”。

5．配置 Internet 验证服务（IAS）

单击“开始”→“管理工具”→“Internet 验证服务”命令，如图 3-23 所示，逐项配置“RADIUS 客户端”、“远程访问记录”、“远程访问策略”、“连接请求处理”等。

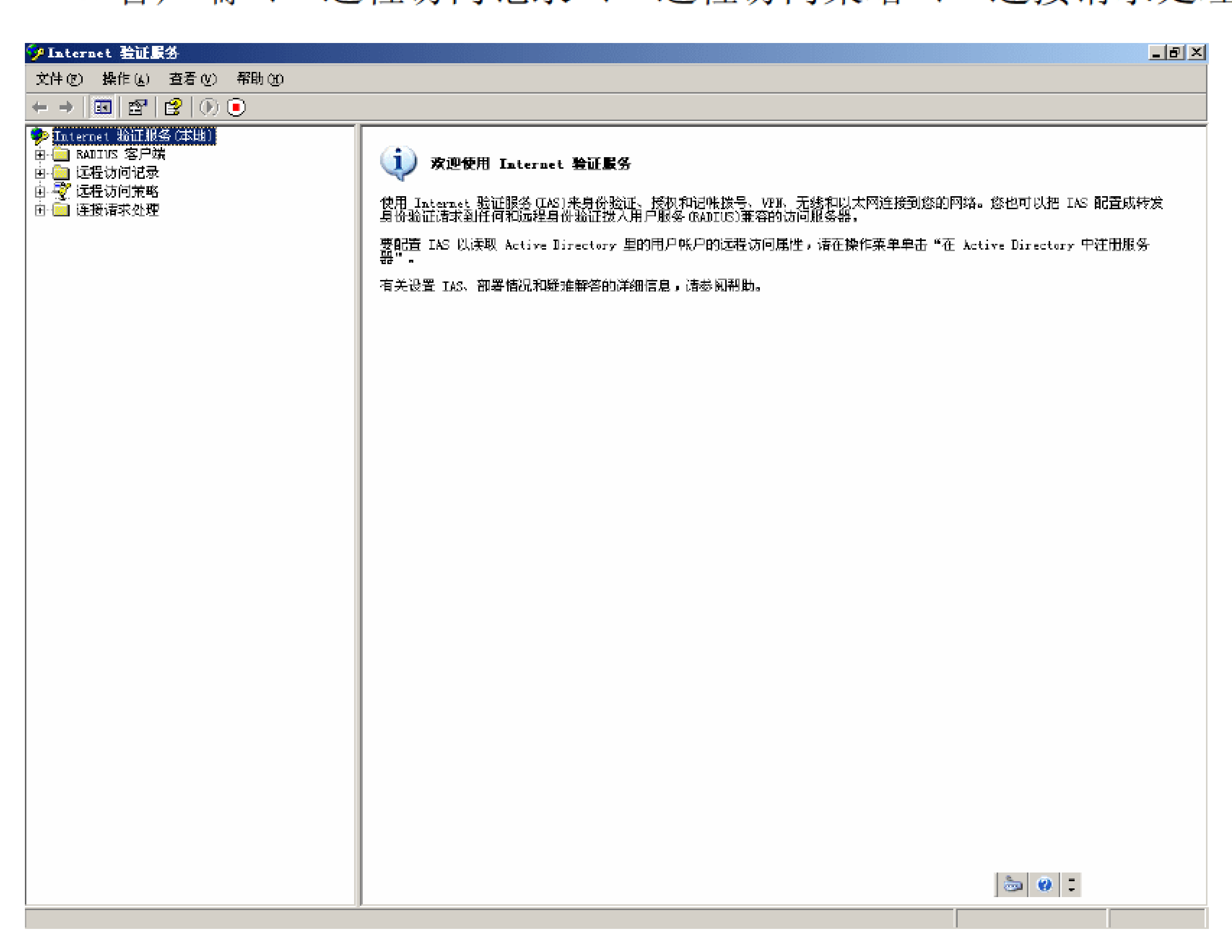


图 3-23　Internet 验证服务

6. 配置“RADIUS 客户端”

在配置环境中就是配置无线接入点（192.168.1.201）。新建 RADIUS 客户端，如图 3-24 和图 3-25 所示。

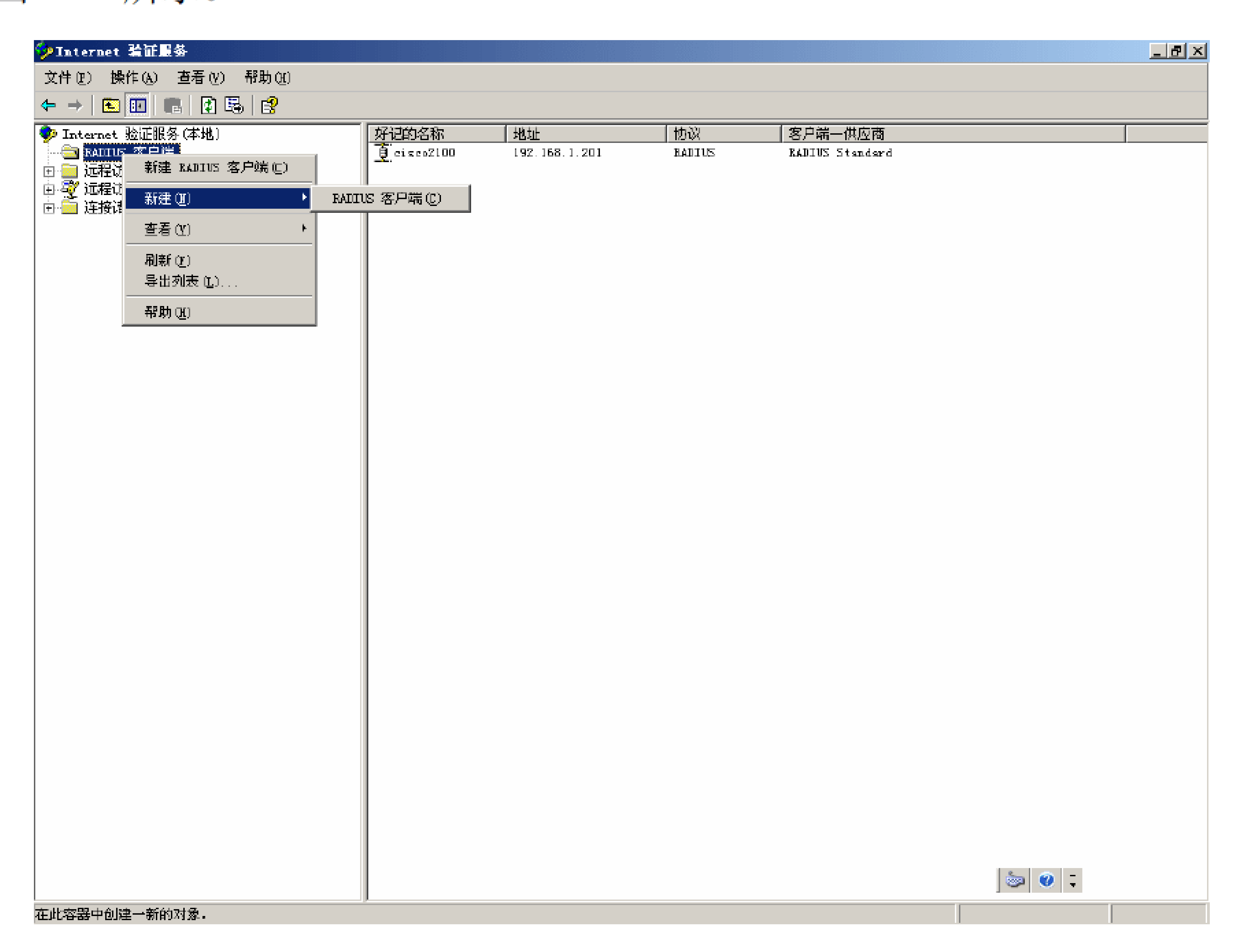


图 3-24 新建 RADIUS 客户端

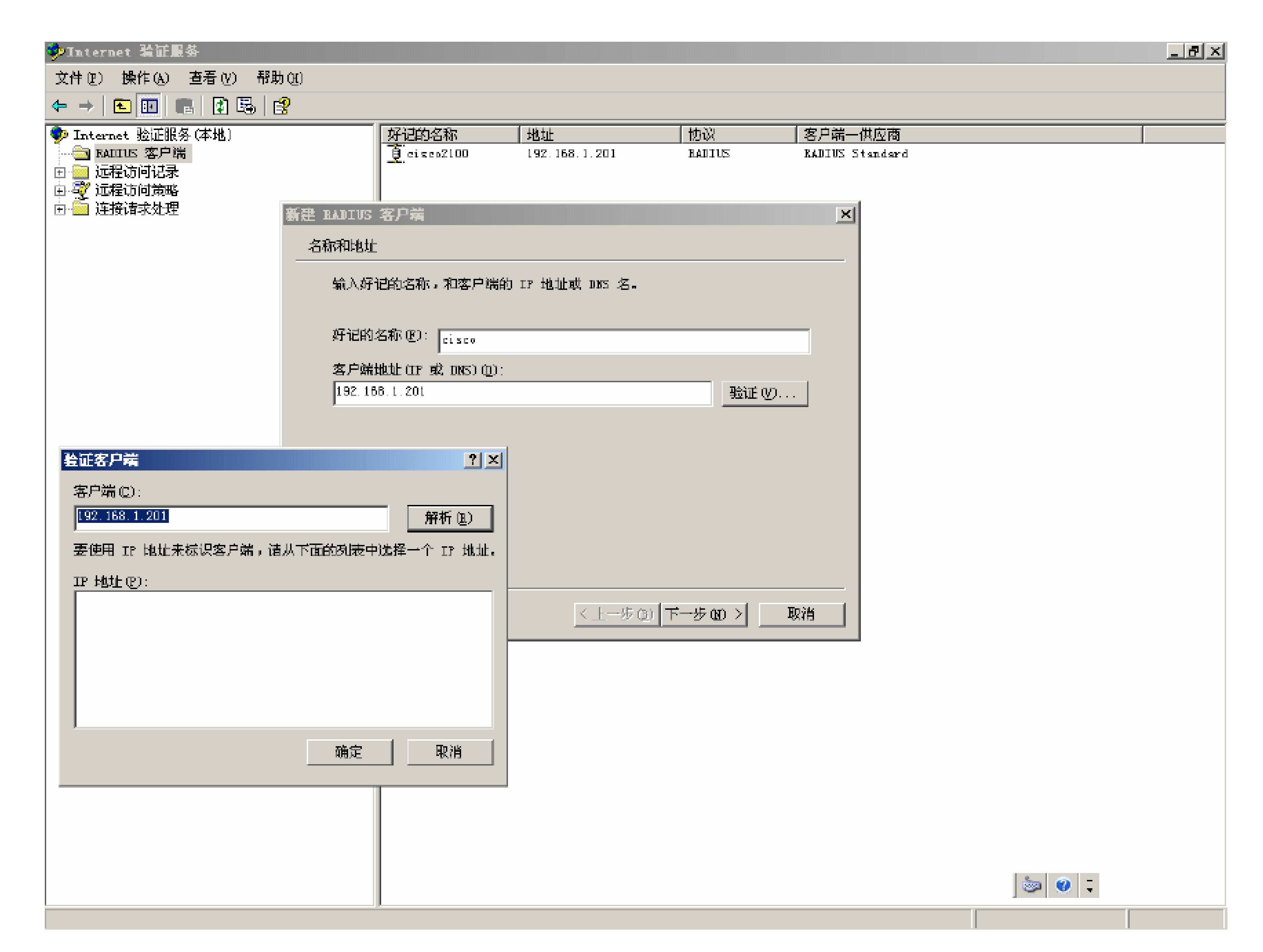


图 3-25 验证客户端

RADIUS 客户端的 IP 地址一定是无线接入点的 IP 地址，这一点最重要。

如图 3-26 所示，“客户端-供应商”一般选择 RADIUS Standard，“共享的机密”中随便输入密码，至此，RADIUS 客户端配置完成。

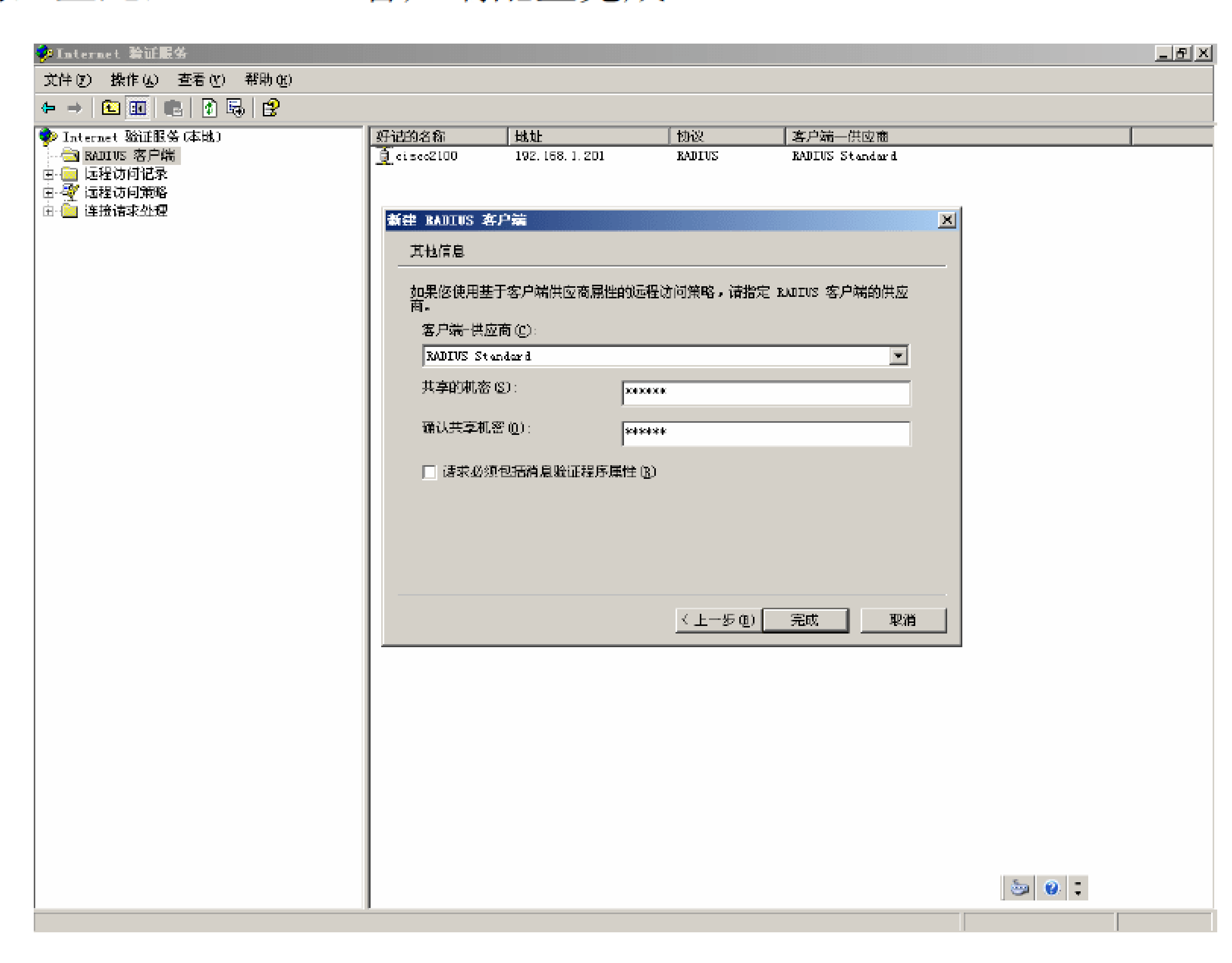


图 3-26　新建 RADIUS 客户端的其他信息

7. 配置“远程访问记录”

左击“远程访问记录”项，在日志记录方法中右击“本地文件”，单击“属性”命令，配置本地文件属性，如图 3-27 所示。

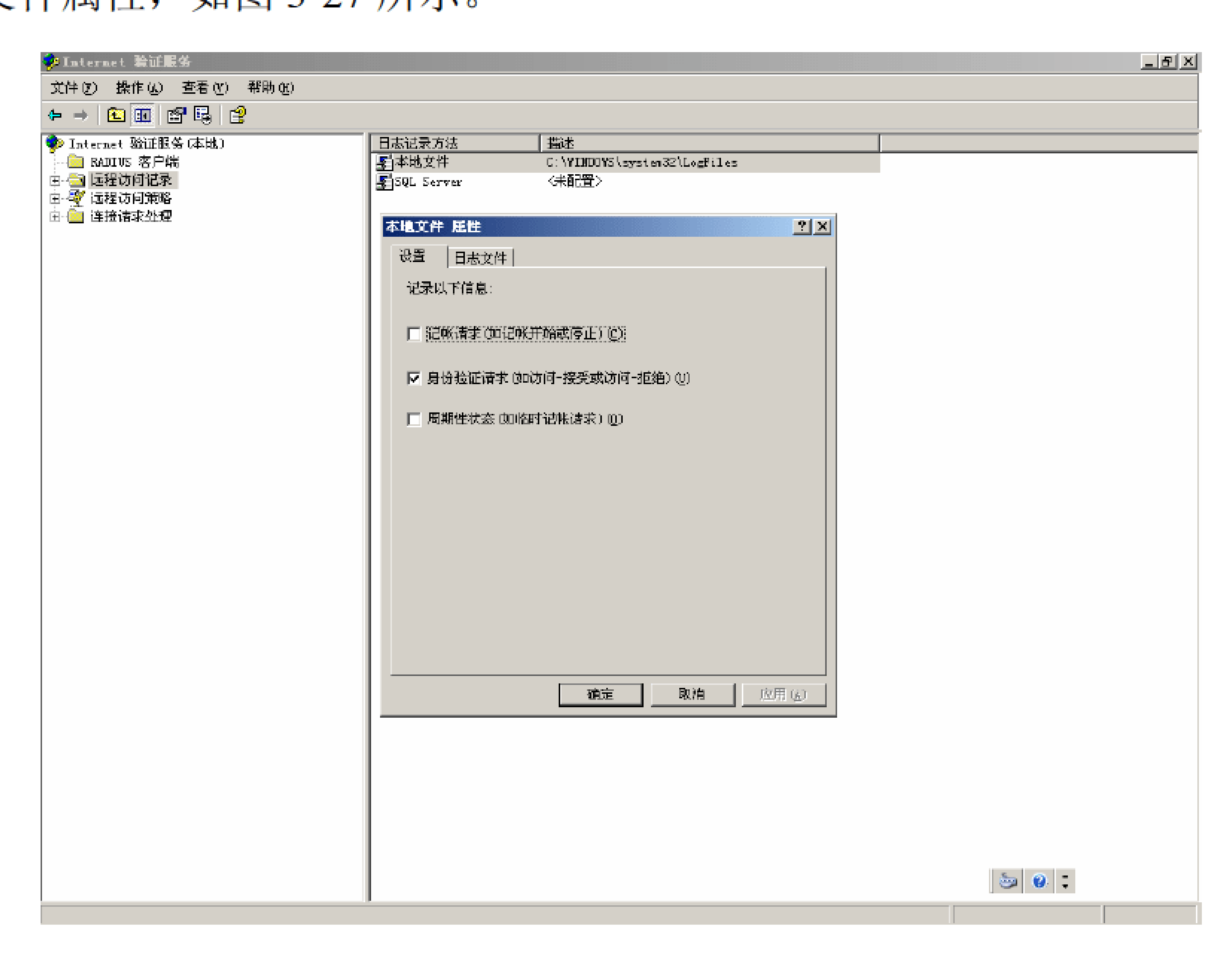


图 3-27　本地文件属性

“设置”选项卡里一般选择“身份验证请求”复选框，如果还要求计账，再选择“记账请求”复选框。

如图 3-28 所示。“日志文件”选项卡里格式选择“IAS”，可以每天创建日志文件，在不用数据库存储日志记录的情况下就不用采用 SQL Server 的日志记录方法了，所以不配置它。关于日志文件里的格式规则（记录 RADIUS 证书验证的各种信息），参看相关帮助。

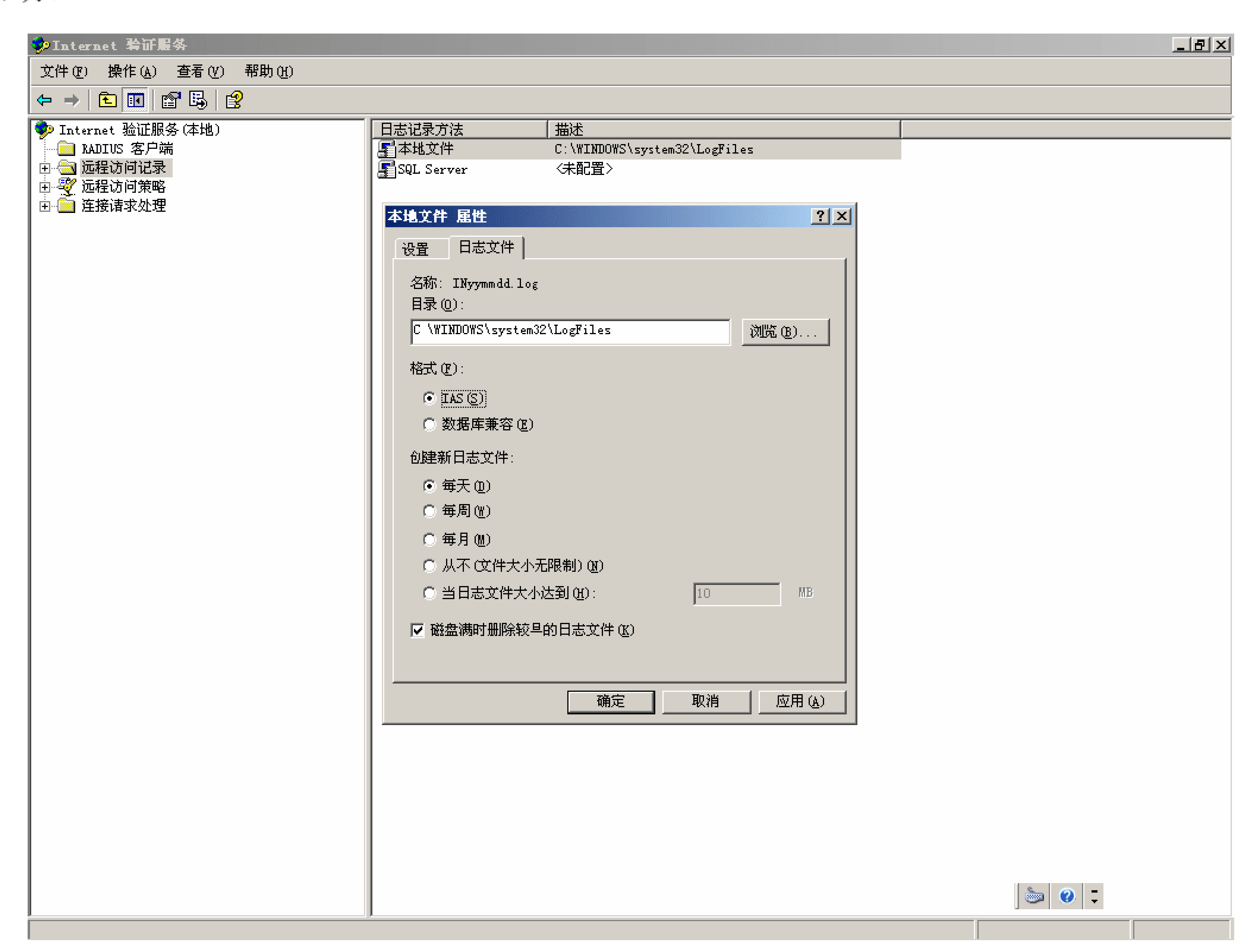


图 3-28　日志文件

客户端证书验证失败的日志记录是一个安全通道事件，默认情况下，在 IAS 服务器上处于未启用状态。将以下注册表项值从“1”（“REG_DWORD”类型，数据“0x00000001”）更改为“3”（“REG_DWORD”类型，数据“0x00000003”），可以启用其他安全通道事件：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogging

至此，“远程访问记录”配置完成。

8．配置“远程访问策略”

新建远程访问策略，如图 3-29 所示。

进入远程访问策略配置向导，如图 3-30 所示，策略名就用好记的字串就可以，如“cisco2100”，访问方法一定要用“无线”，如图 3-31 所示。

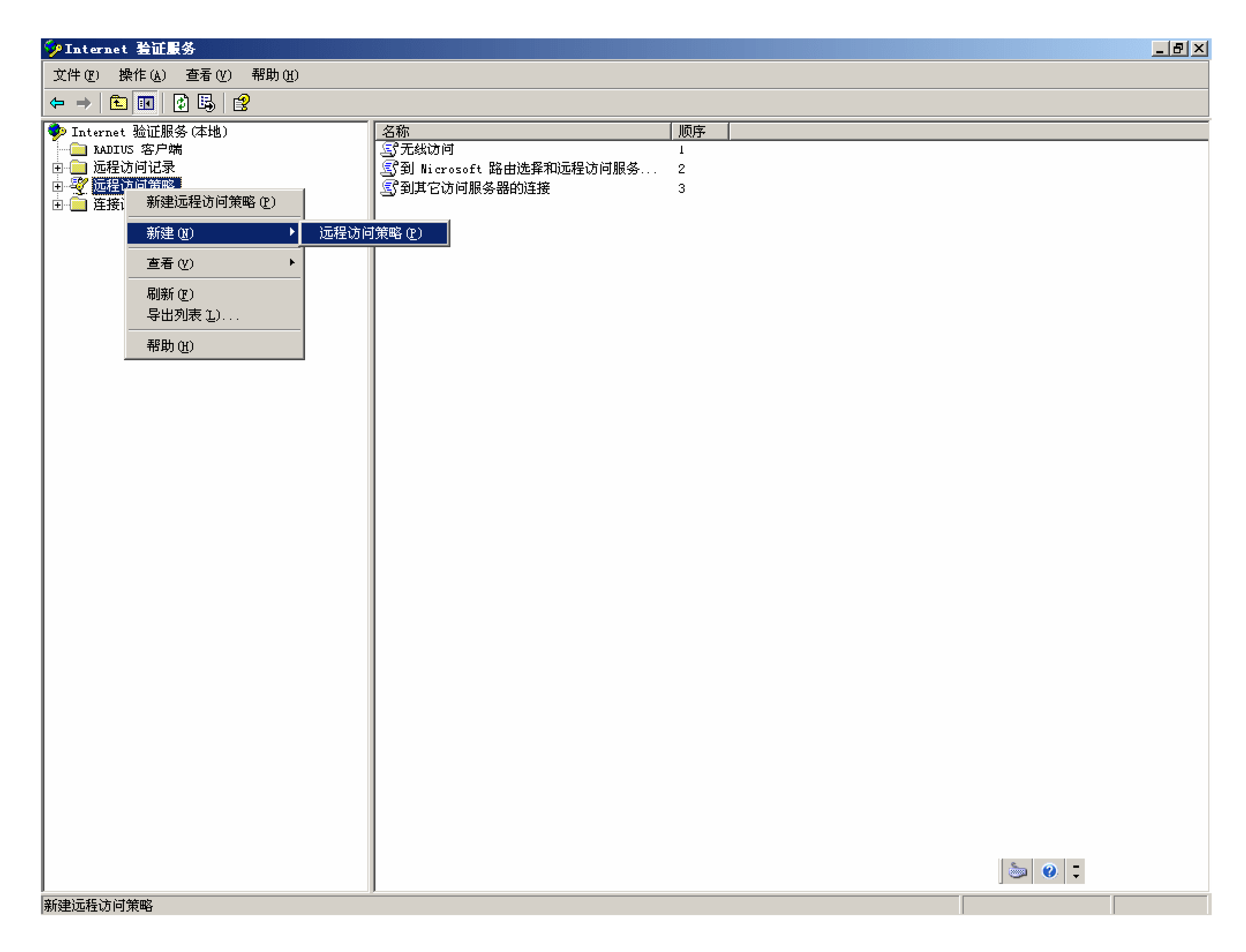


图 3-29　新建远程访问策略

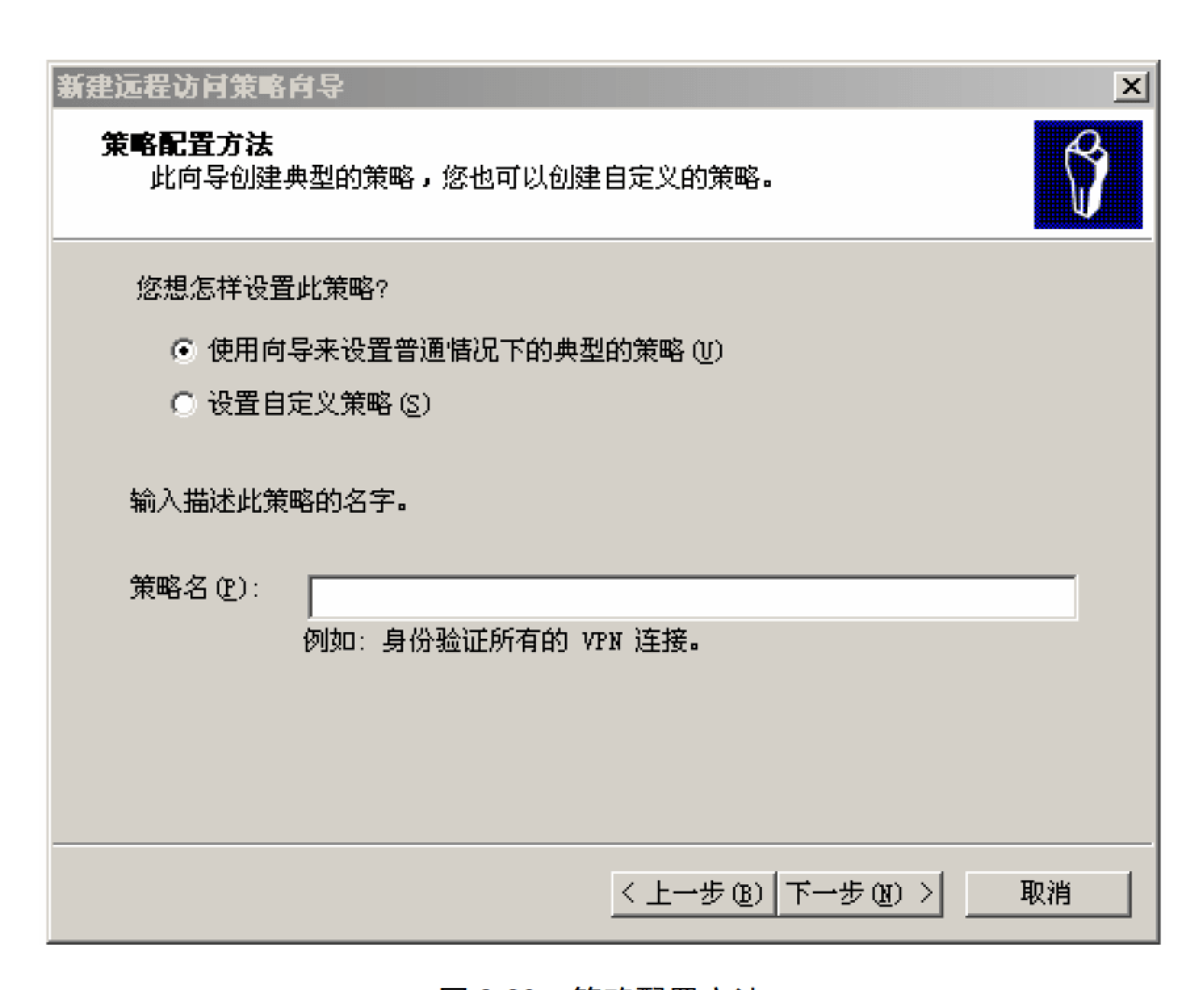


图 3-30　策略配置方法

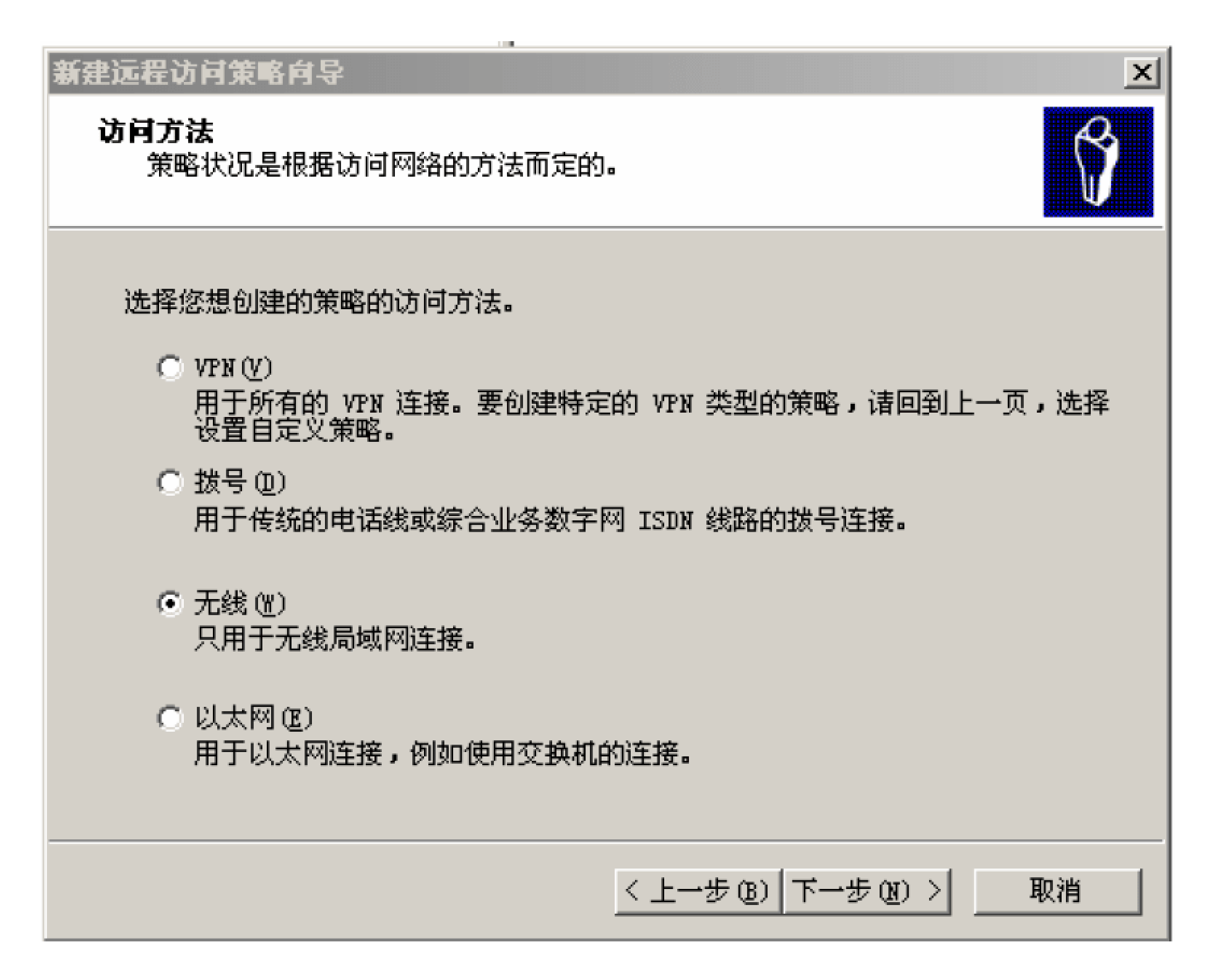


图 3-31 访问方法

给所建的组 test1 授予访问权限，如图 3-32 所示，下面设置身份验证方法，单击“配置”按钮设置 PEAP 的属性，使用 EAP-MSCHAP(V2)，单击“编辑”按钮，身份验证充实次数一般用 2，如图 3-33 所示，单击“确定”按钮。

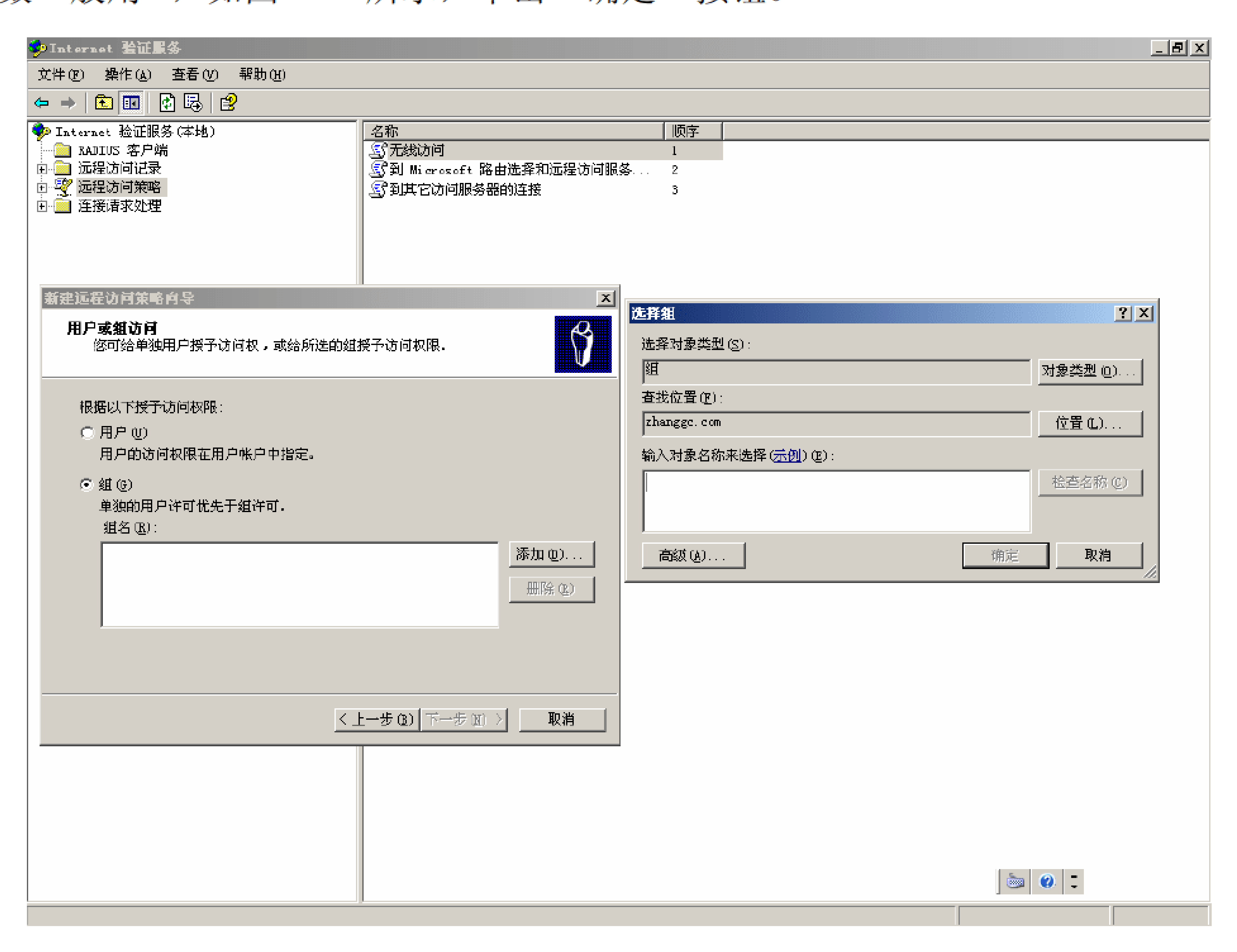


图 3-32 用户或组访问

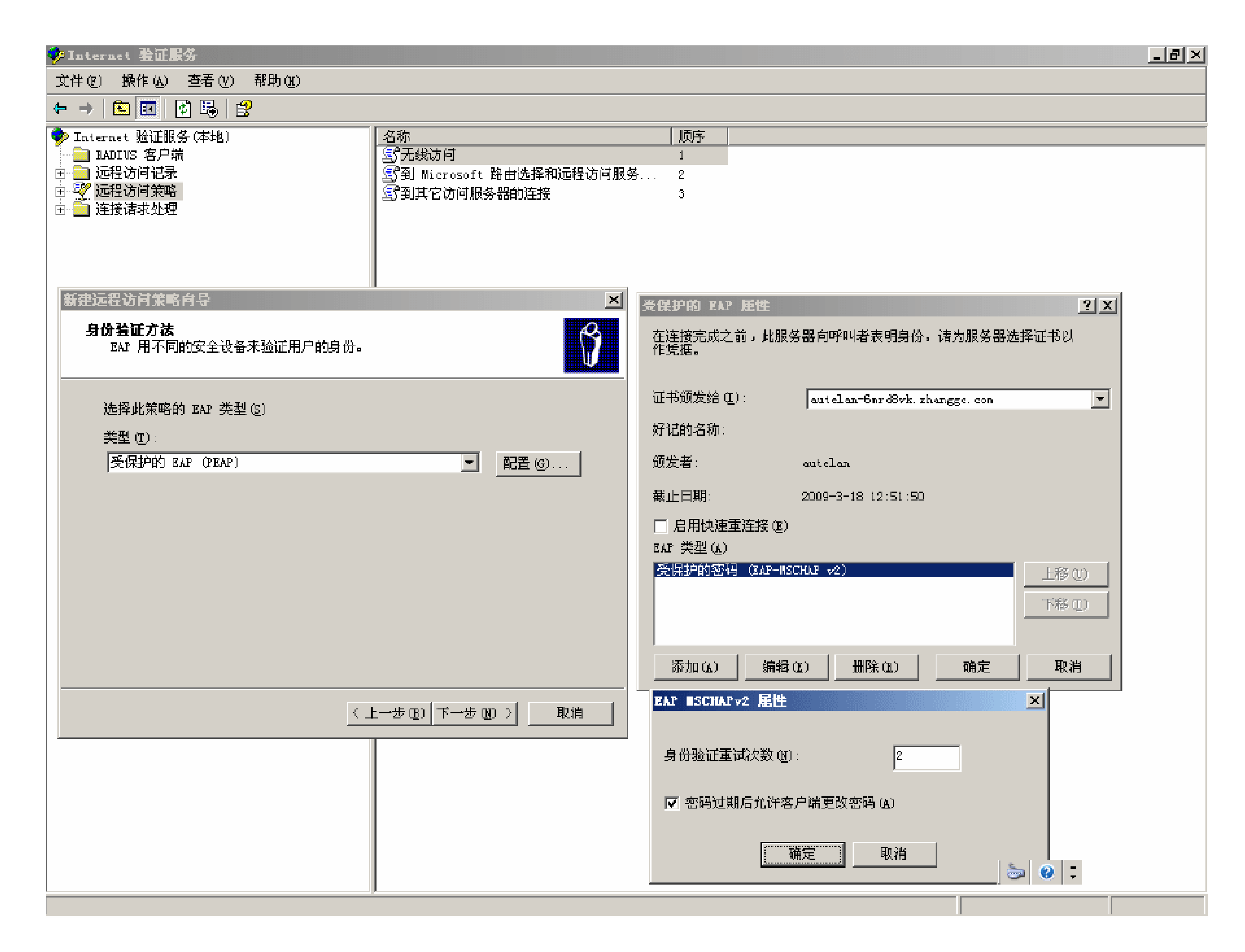


图 3-33　身份验证方法

如图 3-34 所示，单击“完成”按钮，至此远程访问策略设置完毕。

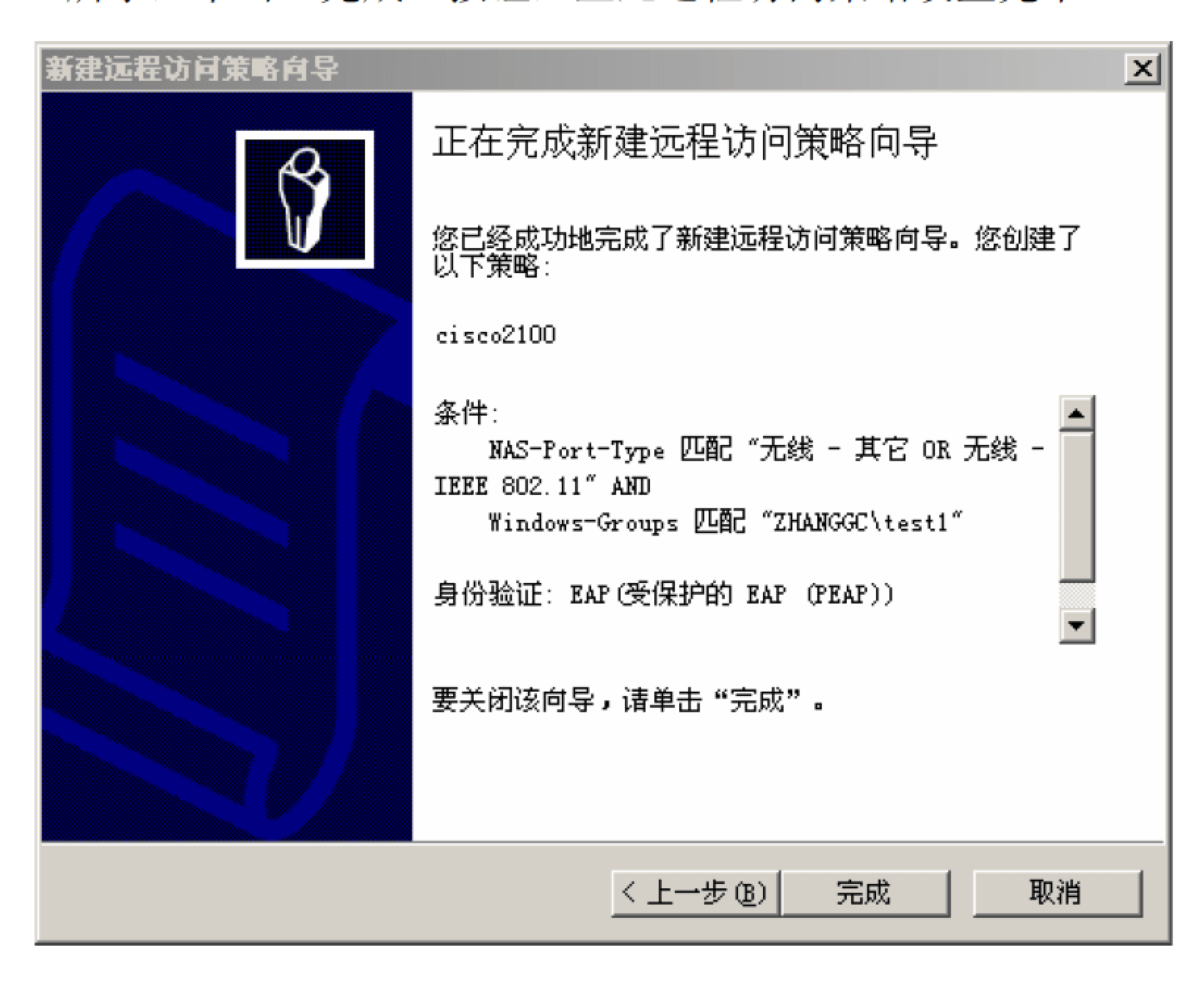


图 3-34　完成新建远程访问策略

9. 配置“连接请求策略”

新建过程如图 3-35 至图 3-39 所示。

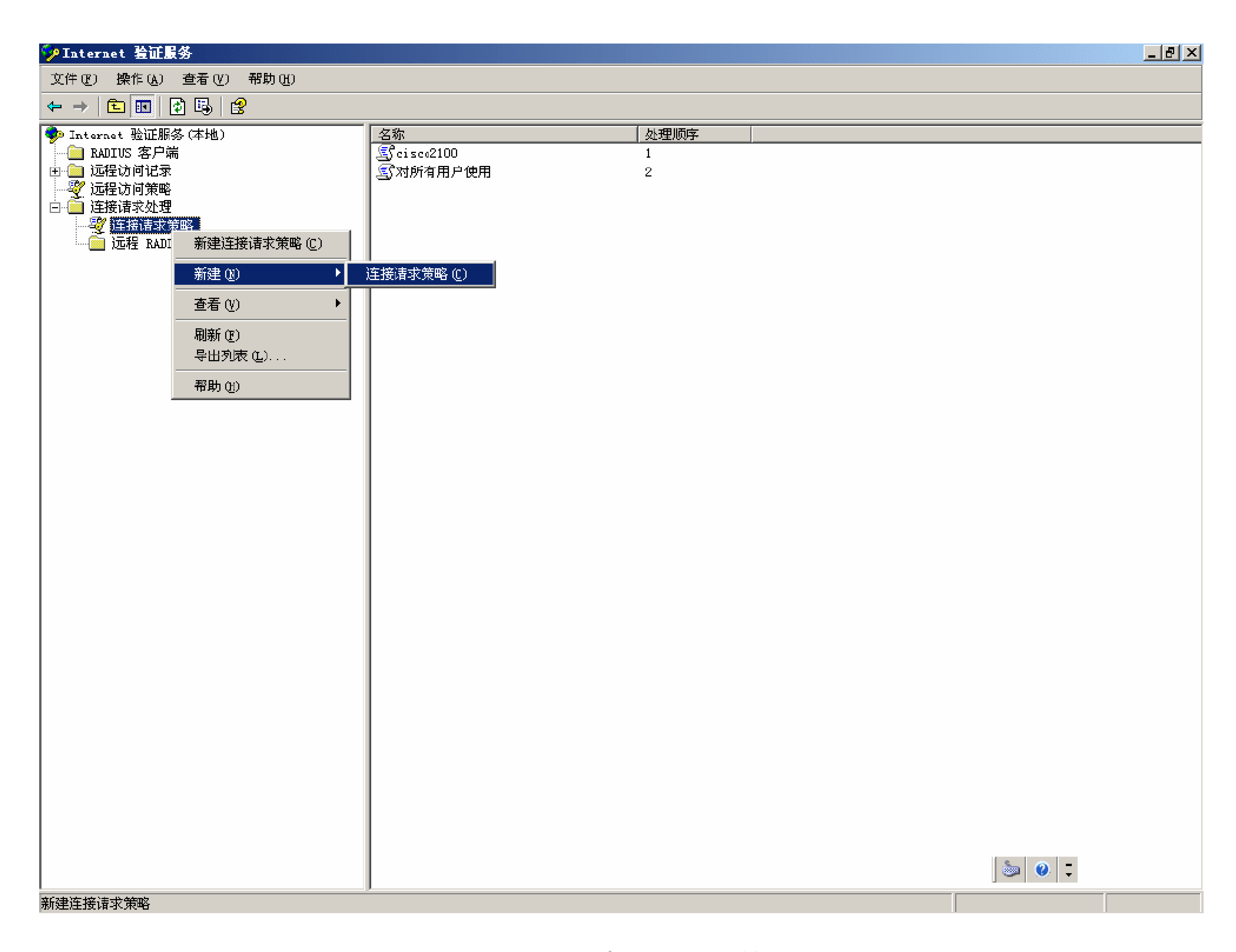


图 3-35　新建连接请求策略



图 3-36　策略配置方法

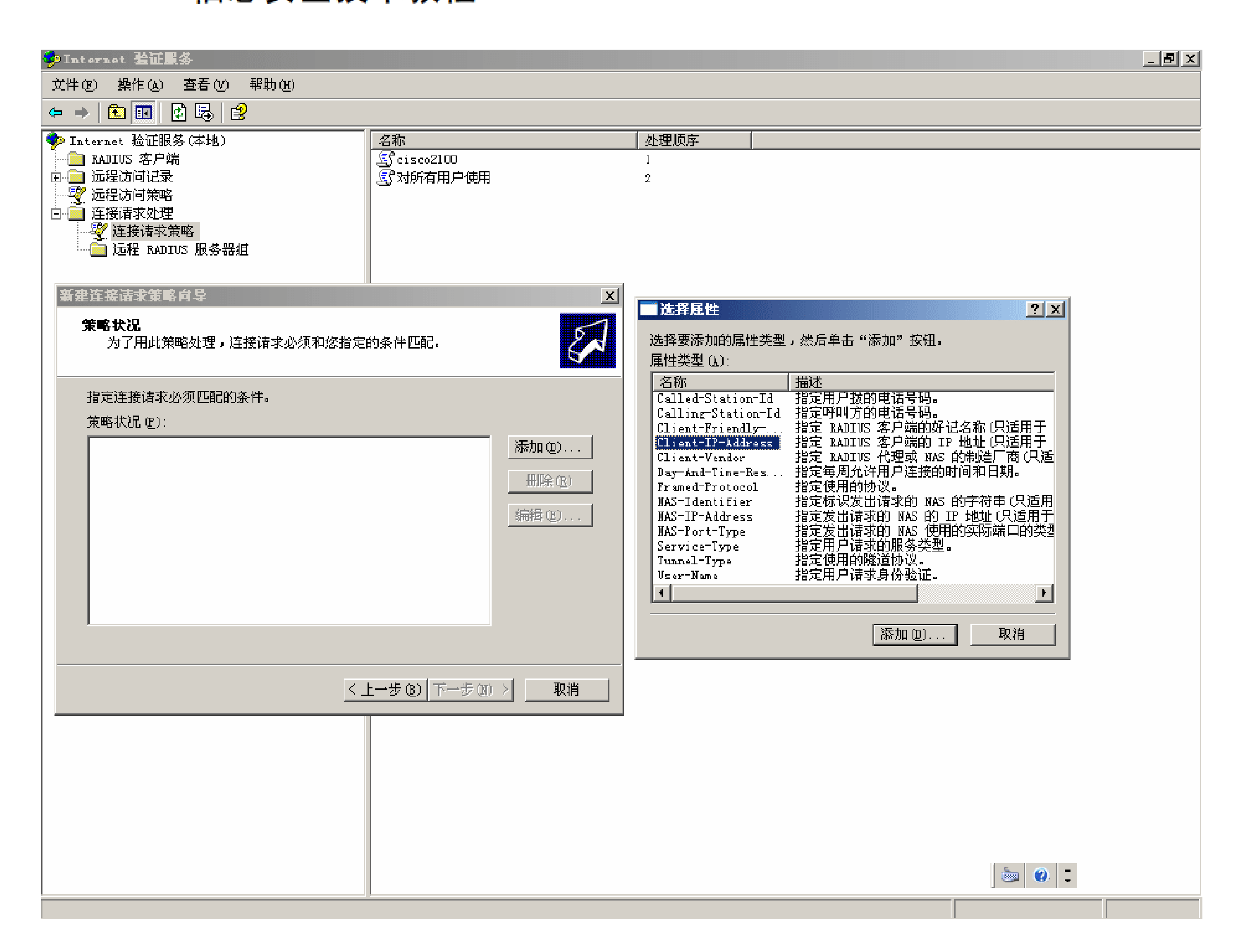


图 3-37 策略状况 1



图 3-38 策略状况 2

至此，连接请求策略配置完成。

10. 配置 IIS（internet 信息服务管理器）

单击“开始”→“管理工具”→“Internet 信息服务管理工具”命令，打开 IIS，展开“网站”，右击“默认网站”，打开默认网站属性，如图 3-40 和图 3-41 所示。

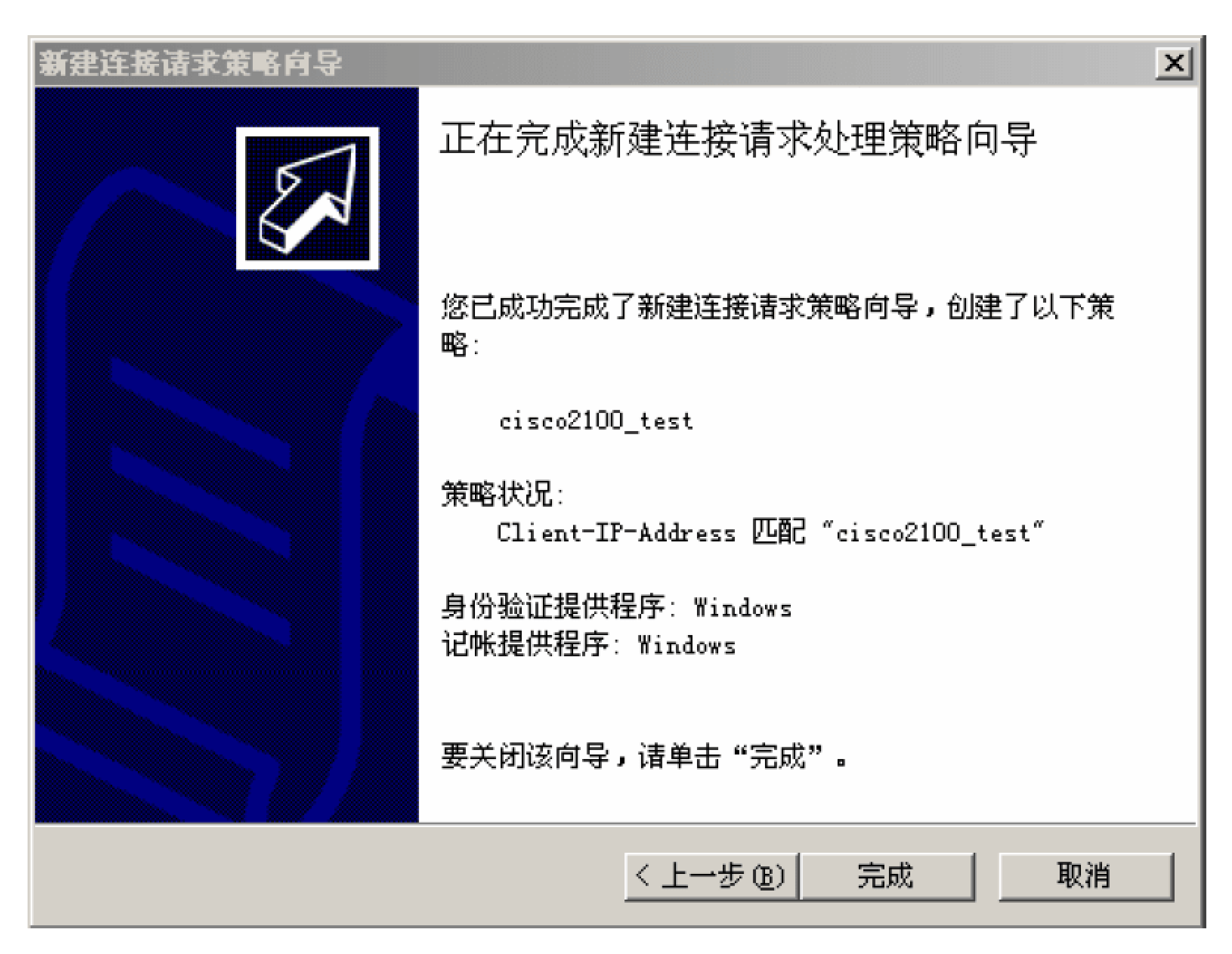


图 3-39 完成新建连接请求处理策略

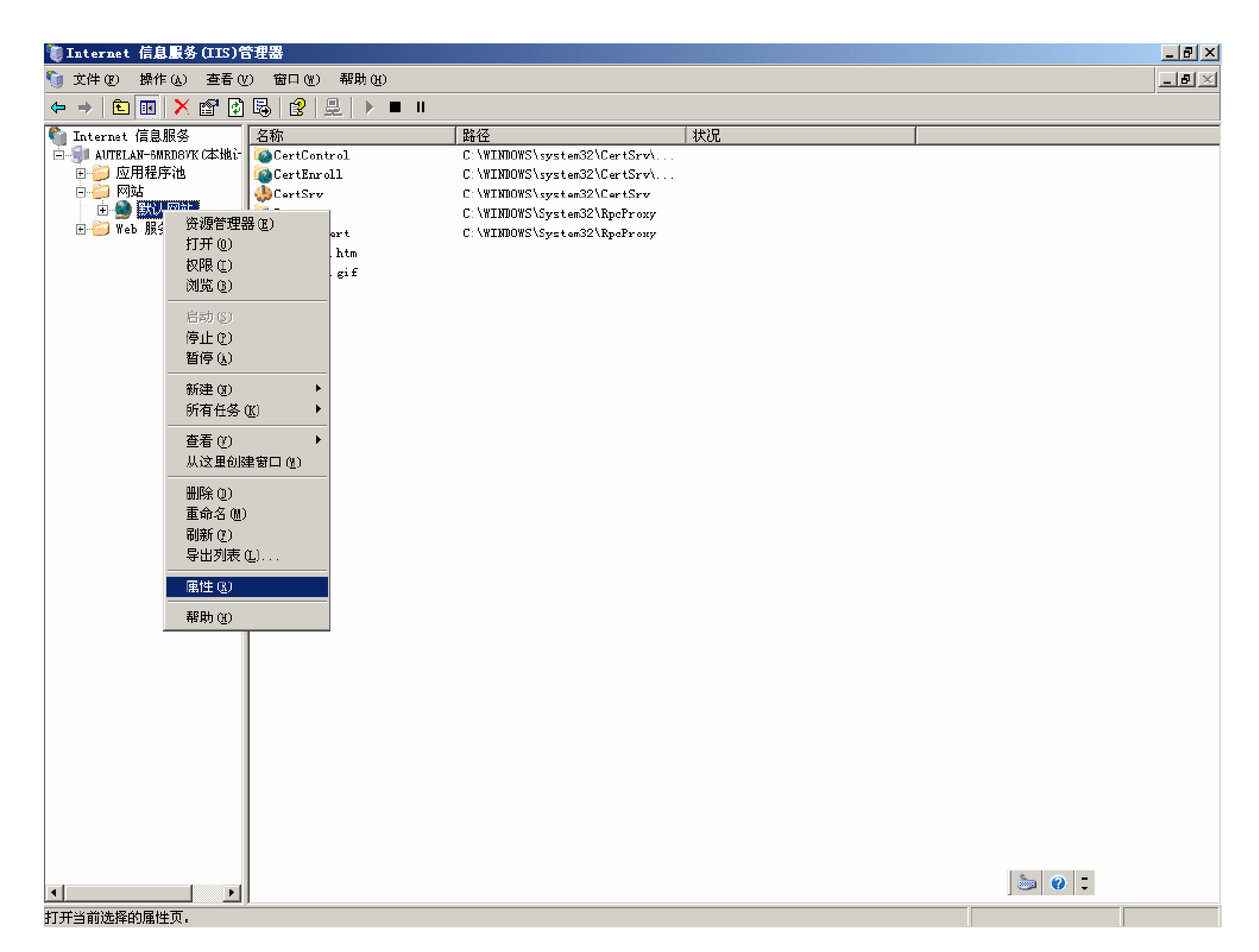


图 3-40 右击“默认网站”

在属性选项卡中选择“目录安全性”选项卡，在“身份验证和访问控制”选项组中单击“编辑”按钮进入“身份验证方法”对话框，如图 3-42 所示。

不要选用“启用匿名访问”，在“用户访问须经过身份验证”对话框中选中“windows 域服务器的摘要式身份验证”复选框，在“领域”栏中选择服务器的根域，如 zhanggc.com，

以后就依次单击“确定”按钮；此属性选项卡中的其他卡项都可以保持默认设置。至此 IIS 设置完毕。

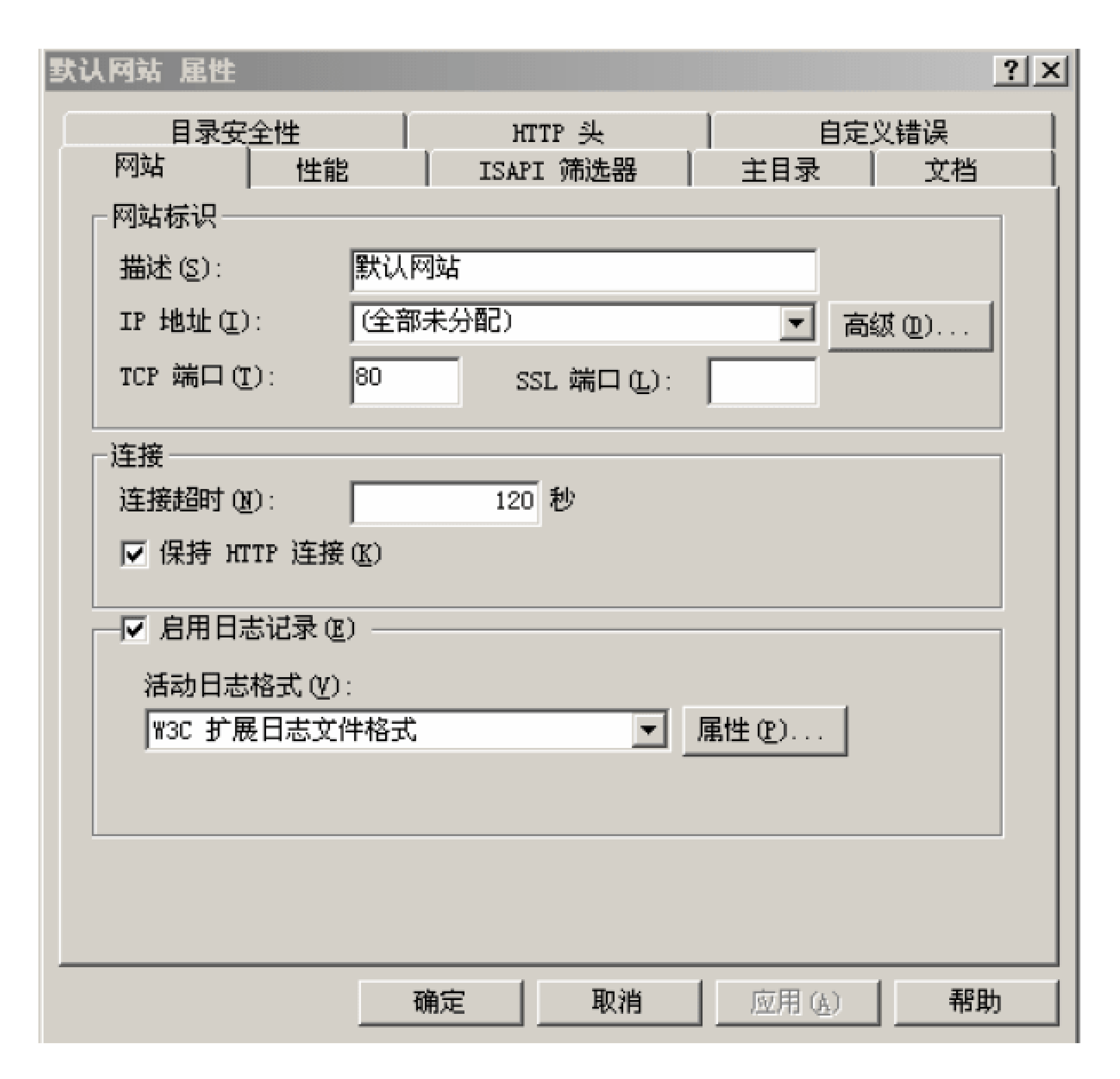


图 3-41　默认网站属性

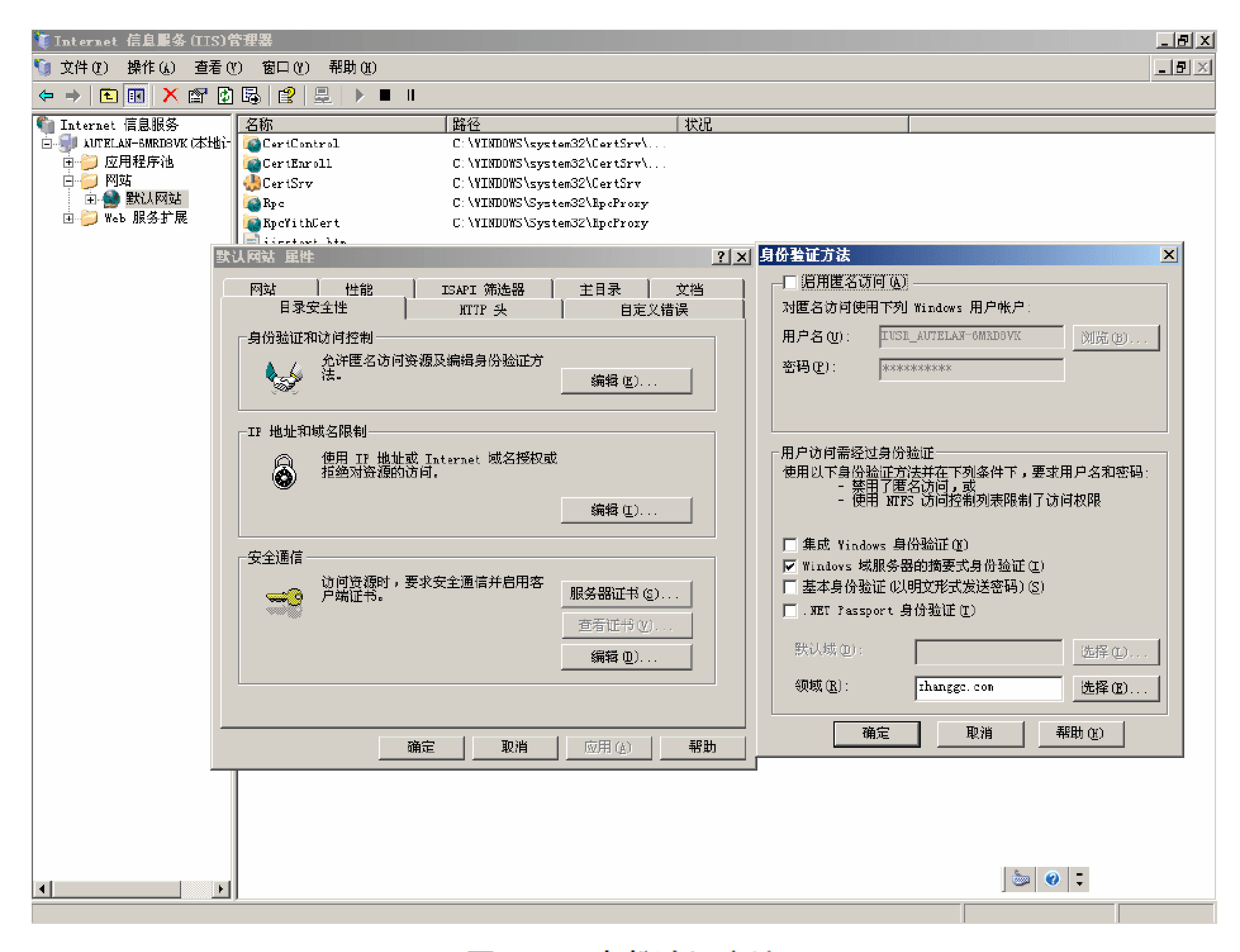


图 3-42　身份验证方法

11．查看记录

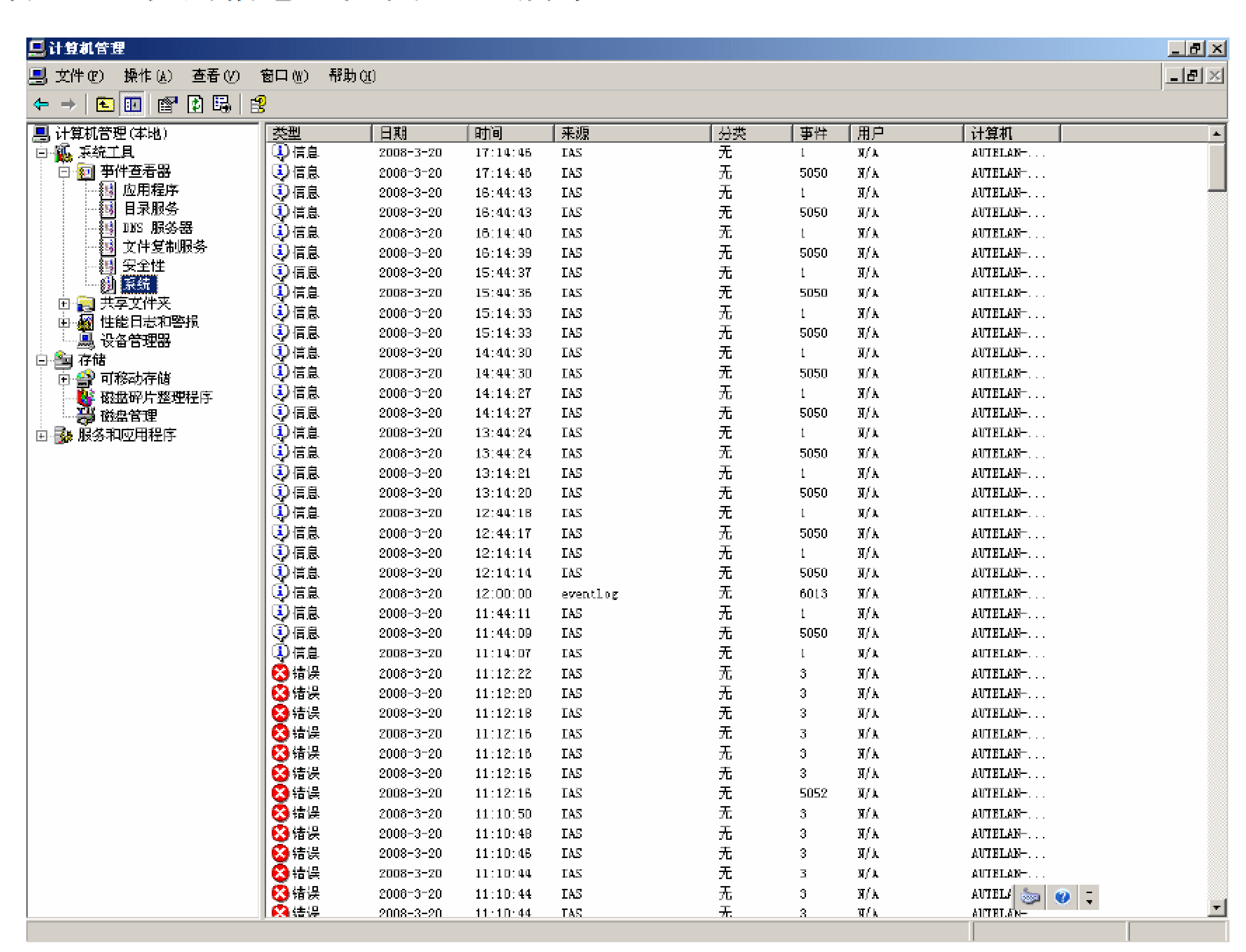
在设置完毕 AD、IAS 和 IIS 这 3 个部件后，RADIUS Server 端的设置算是大功告成，

如果想随时看客户端验证过程的记录信息，可以看远程访问记录，记录文档默认放在C:\WINDOWS\system32\LogFiles 中，其中保存有验证信息，如图 3-43 所示。

```
IN080320.log - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
v2),4127,11,4136,1,4142,0
192.168.1.201,zgc,03/20/2008,14:44:30,IAS,AUTELAN-6MRD8UK,4128,cisco2100,25,311 1 192.168.1.188 03/20/2008 01:08:11 216,4132,
受保护的密码 (EAP-MSCHAP v2),4127,11,8100,0,4120,0x015A48414E4747,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使
用,4129,ZHANGGC\zgc,4149,无线访问,6,2,4130,zhanggc.com/Users/zgc,4136,2,4142,0
192.168.1.201,zgc,03/20/2008,15:14:33,IAS,AUTELAN-6MRD8UK,4128,cisco2100,31,00-1B-77-40-E1-2A,30,00-1D-46-25-E9-
E0:cisco_test1,5,8,4,192.168.1.201,32,CISCO-
2100,26,0x0000376301060000000003,6,2,12,1300,61,19,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使用,4129,ZHANGGC\zgc,4149,
无线访问,25,311 1 192.168.1.188 03/20/2008 01:08:11 227,4130,zhanggc.com/Users/zgc,4132,受保护的密码 (EAP-MSCHAP
v2),4127,11,4136,1,4142,0
192.168.1.201,zgc,03/20/2008,15:14:33,IAS,AUTELAN-6MRD8UK,4128,cisco2100,25,311 1 192.168.1.188 03/20/2008 01:08:11 227,4132,
受保护的密码 (EAP-MSCHAP v2),4127,11,8100,0,4120,0x015A48414E4747,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使
用,4129,ZHANGGC\zgc,4149,无线访问,6,2,4130,zhanggc.com/Users/zgc,4136,2,4142,0
192.168.1.201,zgc,03/20/2008,15:44:37,IAS,AUTELAN-6MRD8UK,4128,cisco2100,31,00-1B-77-40-E1-2A,30,00-1D-46-25-E9-
E0:cisco_test1,5,8,4,192.168.1.201,32,CISCO-
2100,26,0x0000376301060000000003,6,2,12,1300,61,19,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使用,4129,ZHANGGC\zgc,4149,
无线访问,25,311 1 192.168.1.188 03/20/2008 01:08:11 238,4130,zhanggc.com/Users/zgc,4132,受保护的密码 (EAP-MSCHAP
v2),4127,11,4136,1,4142,0
192.168.1.201,zgc,03/20/2008,15:44:37,IAS,AUTELAN-6MRD8UK,4128,cisco2100,25,311 1 192.168.1.188 03/20/2008 01:08:11 238,4132,
受保护的密码 (EAP-MSCHAP v2),4127,11,8100,0,4120,0x015A48414E4747,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使
用,4129,ZHANGGC\zgc,4149,无线访问,6,2,4130,zhanggc.com/Users/zgc,4136,2,4142,0
192.168.1.201,zgc,03/20/2008,16:14:40,IAS,AUTELAN-6MRD8UK,4128,cisco2100,31,00-1B-77-40-E1-2A,30,00-1D-46-25-E9-
E0:cisco_test1,5,8,4,192.168.1.201,32,CISCO-
2100,26,0x0000376301060000000003,6,2,12,1300,61,19,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使用,4129,ZHANGGC\zgc,4149,
无线访问,25,311 1 192.168.1.188 03/20/2008 01:08:11 249,4130,zhanggc.com/Users/zgc,4132,受保护的密码 (EAP-MSCHAP
v2),4127,11,4136,1,4142,0
192.168.1.201,zgc,03/20/2008,16:14:40,IAS,AUTELAN-6MRD8UK,4128,cisco2100,25,311 1 192.168.1.188 03/20/2008 01:08:11 249,4132,
受保护的密码 (EAP-MSCHAP v2),4127,11,8100,0,4120,0x015A48414E4747,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使
用,4129,ZHANGGC\zgc,4149,无线访问,6,2,4130,zhanggc.com/Users/zgc,4136,2,4142,0
192.168.1.201,zgc,03/20/2008,16:44:43,IAS,AUTELAN-6MRD8UK,4128,cisco2100,31,00-1B-77-40-E1-2A,30,00-1D-46-25-E9-
E0:cisco_test1,5,8,4,192.168.1.201,32,CISCO-
2100,26,0x0000376301060000000003,6,2,12,1300,61,19,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使用,4129,ZHANGGC\zgc,4149,
无线访问,25,311 1 192.168.1.188 03/20/2008 01:08:11 260,4130,zhanggc.com/Users/zgc,4132,受保护的密码 (EAP-MSCHAP
v2),4127,11,4136,1,4142,0
192.168.1.201,zgc,03/20/2008,16:44:43,IAS,AUTELAN-6MRD8UK,4128,cisco2100,25,311 1 192.168.1.188 03/20/2008 01:08:11 260,4132,
受保护的密码 (EAP-MSCHAP v2),4127,11,8100,0,4120,0x015A48414E4747,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使
用,4129,ZHANGGC\zgc,4149,无线访问,6,2,4130,zhanggc.com/Users/zgc,4136,2,4142,0
192.168.1.201,zgc,03/20/2008,17:14:46,IAS,AUTELAN-6MRD8UK,4128,cisco2100,31,00-1B-77-40-E1-2A,30,00-1D-46-25-E9-
E0:cisco_test1,5,8,4,192.168.1.201,32,CISCO-
2100,26,0x0000376301060000000003,6,2,12,1300,61,19,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使用,4129,ZHANGGC\zgc,4149,
无线访问,25,311 1 192.168.1.188 03/20/2008 01:08:11 271,4130,zhanggc.com/Users/zgc,4132,受保护的密码 (EAP-MSCHAP
v2),4127,11,4136,1,4142,0
192.168.1.201,zgc,03/20/2008,17:14:46,IAS,AUTELAN-6MRD8UK,4128,cisco2100,25,311 1 192.168.1.188 03/20/2008 01:08:11 271,4132,
受保护的密码 (EAP-MSCHAP v2),4127,11,8100,0,4120,0x015A48414E4747,4108,192.168.1.201,4116,0,4155,1,4154,对所有用户使
用,4129,ZHANGGC\zgc,4149,无线访问,6,2,4130,zhanggc.com/Users/zgc,4136,2,4142,0
```

图 3-43　远程访问记录

还可以按以下方式打开：右击桌面的“我的电脑”图标，选择“管理”命令，打开“计算机管理”窗口，展开“系统工具”中的“事件查看器”，单击“系统”项，可以查看客户端验证过程的信息，如图 3-44 所示。



类型	日期	时间	来源	分类	事件	用户	计算机
信息	2008-3-20	17:14:46	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	17:14:46	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	16:44:43	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	16:44:43	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	16:14:40	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	16:14:39	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	15:44:37	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	15:44:36	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	15:14:33	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	15:14:33	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	14:44:30	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	14:44:30	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	14:14:27	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	14:14:27	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	13:44:24	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	13:44:24	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	13:14:21	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	13:14:20	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	12:44:18	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	12:44:17	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	12:14:14	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	12:14:14	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	12:00:00	eventlog	无	6013	N/A	AUTELAN-...
信息	2008-3-20	11:44:11	IAS	无	1	N/A	AUTELAN-...
信息	2008-3-20	11:44:09	IAS	无	5050	N/A	AUTELAN-...
信息	2008-3-20	11:14:07	IAS	无	1	N/A	AUTELAN-...
错误	2008-3-20	11:12:22	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:12:20	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:12:18	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:12:16	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:12:16	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:12:16	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:12:16	IAS	无	5052	N/A	AUTELAN-...
错误	2008-3-20	11:10:50	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:10:48	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:10:46	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:10:44	IAS	无	3	N/A	AUTELAN-...
错误	2008-3-20	11:10:44	IAS	无	3	N/A	AUTEL
错误	2008-3-20	11:10:44	IAS	无	3	N/A	AUTELAN-

图 3-44　客户端验证过程信息

第4章　安全协议

本章学习重点：

- 传输控制协议（TCP）和网际协议（IP）在网络中的作用
- TCP/IP 协议簇中的重要协议及工作原理
- TCP/IP 数据包格式
- 通过 IPSec 增强网络安全性
- 安全协议介绍

众多计算机网络，包括 Internet 本身都是通过 TCP/IP 协议进行交互。TCP/IP 协议中，最为关键的两个组件——传输控制协议（TCP）和网际协议（IP），控制着网络上端口与端口之间网络数据的格式与路由。本章重点论述 TCP/IP，因为 TCP/IP 是最为通用的通信协议，因而也必然存在大量安全漏洞。

4.1 TCP/IP 工作原理

TCP/IP 协议并不完全符合 OSI 的七层参考模型，其采用了 4 层的层次结构，其中每一层执行一特定任务。该模型的目的是使硬件在相同的层次上相互通信，每一层都由下一层提供的服务完成本层的需求，并向上一层提供服务。这 4 层分别为应用层、传输层、网络层、网络接口层。图 4-1 给出了 OSI 体系结构和 TCP/IP 体系结构的对应关系。

OSI的体系结构

7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层

（a）

TCP/IP的体系结构

应用层（各种应用层协议，如SMIPP，TELNET，FTP等）
传输层（UDP或TCP）
网际导IP
网络接口层

（b）

图 4-1　OSI 体系结构和 TCP/IP 体系结构

- ❑ **应用层**　体系结构的最高层，应用层直接为用户的应用进程提供服务。这一层的协议包括简单邮件传输协议（SMTP）、文件传输协议（FTP）、网络远程访问协议（Telnet）等。
- ❑ **传输层**　这一层负责向两个主机的进程之间的通信提供服务，主要功能是数据格式化、数据确认和丢失重传等。这一层的协议包括传输控制协议（TCP）、用户数据报协议（UDP）。
- ❑ **网络层**　负责为不同主机之间提供基本的数据封包传送功能，通过路由选择功

能使得每一个数据包都能准确到达目的主机（但不检查是否被正确接收）。这一层的协议主要是网际协议（IP）。

- **网络接口层（主机—网络层）** 从网络上接收物理帧，并从帧中抽取 IP 数据报转交给网络层，或者将从网络层接收的数据包从过物理网络发送，同时定义如何使用实际网络（如 Ethernet、Serial Line 等）来传送数据。

图 4-2 给出了 TCP/IP 中数据的流动过程。假设主机 A 的应用进程 P_1 与主机 B 的应用进程 P_2 进行通信，主机 A 首先将应用程序数据交给本机的应用层，在应用层加上应用层头部（头部中包含了必要的控制信息）构成下一层的数据单元，然后向下传递给传输层。传输层收到上一层数据后，加上本层的头部构成下一层的数据单元，然后向下传递给网络层。以此类推，数据到达物理层之后，以比特流的形式在物理层上进行传播。当比特流经过网络传播到达主机 B 时，就从最底层向上传播至应用层。每一层根据控制信息进行必要的操作，然后将控制信息剥去，将该层剩下的数据单元上交给更高一层。最后，把应用进程 P_1 发送的数据交给目的主机的应用进程 P_2。

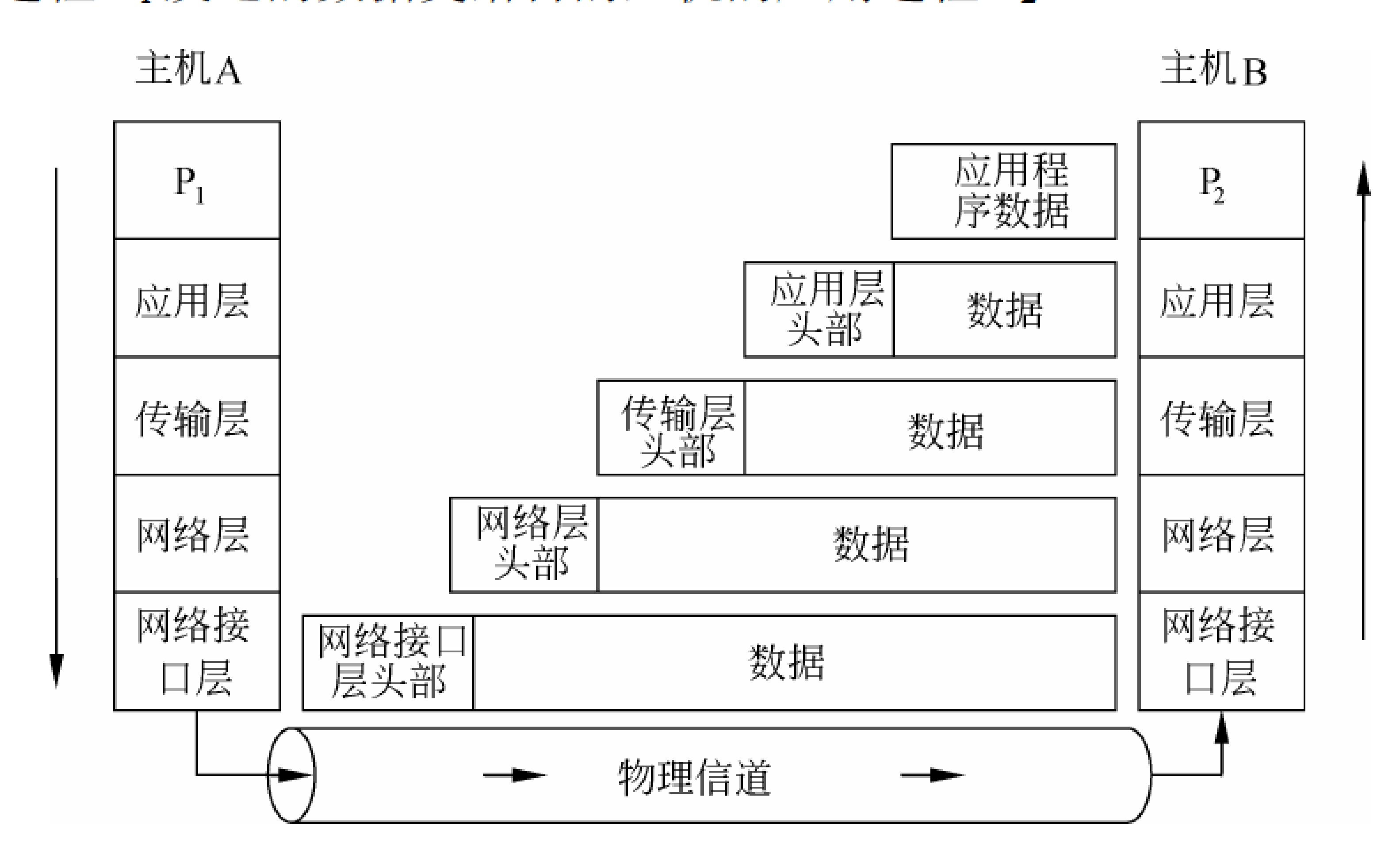


图 4-2　TCP/IP 工作原理

TCP/IP 协议

TCP/IP 协议中的 4 种核心协议是网际协议（IP）、传输控制协议（TCP）、用户数据报协议（UDP）和控制报文协议（ICMP），这 4 种协议是 TCP/IP 网络通信的基础。

1. IP 协议

网际协议在 TCP/IP 中为数据包提供路由功能，每个连接网络的终端设备都有唯一的 IP 来标识自己。

IP 协议也规定网络设备该如何处理接收的数据包，每一个 IP 数据包内都含有一个目的 IP 和源 IP。当网络设备接收到数据包时，首先检查数据包的目的 IP 是否与自己的 IP 一致，如果一致，就在本地运行数据包；如果不一致，就要决定数据包下一跳的位置以便于其到达目的地，IP 协议就是保证系统能够有效地决定下一跳的位置使得所有的网络

流量都可以到达目的地址。

IP 协议的另一个作用是数据包分段。网络中的数据包，在从其源地址到目的地址的途中，会通过很多具有不同拓扑结构的中间网络，每个中间网络允许的最大数据包的长度是不一样的，所以 IP 协议就必须通过分段来保证数据包在到达目的地前能满足各个网络的最大长度的限制。如果一个网络接收到了一个比它最大长度还要长的数据包，IP 协议就可以将这个数据包分成两个或两个以上的段落。

2．传输控制协议（TCP）

TCP 为网络提供可靠的端到端通信，运行在 IP 之上。

TCP 有以下 3 个核心功能。

（1）TCP 是一个可靠的端到端传输协议，当一个系统成功地收到数据包的时候，会反馈一个确认报文表示。

（2）TCP 提供差错检测，每一个数据包都包含一个校验和，当接收方接到数据包后会使用这个校验和来验证该数据包是否在传输过程中被更改。如果校验和与数据不匹配，那么接收方就会要求发送方重新发送。

（3）TCP 是面向连接的，每次通信前，通信的双方会首先通过会话建立和撤销算法在两者之间建立专用的信道。

TCP 保证数据完整，无损并按顺序到达，同时其不断的测试网络的负载来控制数据发送的数据。但在高丢包率或要求实时的网络中，TCP 的这些特点可能会成为其短板。

3．用户数据报协议（UDP）

UDP 协议是一个面向无连接的数据包协议，与 TCP 工作在一个层，是一个不可靠的协议。UDP 不检查数据是否到达目的地，相对于 TCP，UDP 协议不能保证数据按顺序到达，所以其更适合一些实时、高速的网络。

4．控制报文协议（ICMP）

为了提高 IP 数据包交付成功的机会，互联网在网络层使用 ICMP 协议。ICMP 允许主机或路由器报告差错情况和有关异常情况。ICMP 是 IP 层的协议，ICMP 报文作为 IP 层数据包的数据，加上数据包的首部，组成 IP 分组发送出去。

4.2 TCP/IP 协议安全

TCP/IP 网络内部存在着大量的安全漏洞。众所周知，TCP/IP 最初是为部分相互信任的计算机之间的通信而设计的，所以在设计之初并未考虑安全问题，随着网络规模的扩大，安全问题日益突显。

安全专家们在架构中加入了大量的安全机制，这些安全协议在协议框架里工作的位置如下列所示。

应用层安全——S/MIME、Web 安全、SET、Kerberos

传输层安全——SSL、TLS

网络层安全——IPSec、VPNs
链路层安全——PPP、RADIUS

4.2.1 S/MIME

S/MIME（Secure/Multipurpose Internet Mail Extensions）是多用途网络邮件扩充协议（MIME）的扩充，其中加入了数字签名并对邮件内容进行了加密。在 S/MIME 之前，广泛接受的电子邮件协议是 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）。由于 SMTP 内在的原因（其开发的最初目的是在封闭的网络中传送相对来说不太重要的简短邮件，而不是为了在互联网中传送重要而敏感的信息）而缺乏安全性，或者需要使用更安全且专用的解决方案，但选择解决方案时或者着眼于安全性，或者着眼于连接性。而使用 S/MIME 时，则可选择使用既安全又被广泛接受的电子邮件。

MIME 协议是一个网络通信协议，用于规范多媒体数据的传输，包括图片、音频和视频。在 RCF1521 中对其有详细介绍。当 Web 站点将文件发送给客户端浏览器的时候，就会在文档前面加上 MIME 头，然后进行传输。整个文件包含两部分：头部和身体。对于头部来说，又分为两个部分：MIME type 和 subtype。MIME type 描述给该文档要传输的内容的类型，如图像、文本、音频、引用程序等，而 subtype 就是具体的文件类型，如 jpeg、gif、tiff 等。

S/MIME 就是在 MIME 的基础上增加了安全服务——加密和数字证书。加密提供了 3 种加密算法（Diffie-Hallman、RSA、三层 DES）进行会话密钥的加密，创建数字证书的时候，S/MIME 会使用 160 位的 SHA-1 或 MD5 等 Hash 函数来生成消息摘要，并使用 DSS 或 RSA 对消息摘要进行加密而形成数字证书。

S/MIME 是与 SMTP 同样重要的一个标准，因为它将 SMTP 带入了一个新的层次：既能实现广泛的电子邮件连接性，又不会破坏安全性。

1. S/MIME 的历史

1995 年，众多安全供应商于开发出了年第一版 S/MIME。当时，安全邮件并没有公认的单一标准，只有几个相互竞争的标准。第一版 S/MIME 是实现邮件安全性的几个规范之一，其他的规范如 Pretty Good Privacy（PGP），是实现邮件安全性的另一个规范。

1998 年，第 2 版 S/MINE（即 S/MIME 2）开始推出。与版本 1 不同的是，基于希望成为 Internet 标准的考虑，S/MIME 2 被提交到 Internet 工程任务组（IETF）。因而，S/MIME 从众多可能的标准中脱颖而出，从而成为邮件安全标准的领跑者。S/MIME 2 由两份 IETF 征求意见文档（RFC）组成。

（1）建立邮件标准的 RFC 2311 (http://www.ietf.org/rfc/rfc2311.txt)。

（2）建立证书处理标准的 RFC 2312 (http://www.ietf.org/rfc/rfc2312.txt)。

这两份征求意见文档共同提供了第一个基于 Internet 标准的框架，供应商可以按照该框架来提出可互操作的邮件安全解决方案。从此，S/MIME 开始成为邮件安全的标准。

1999 年，为了增强 S/MIME 的 功能，IETF 提议使用 S/MIME 版本 3。在 RFC 2311 基础上，建立了 RFC 2632 (http://www.ietf.org/rfc/rfc2632.txt)，指定 S/MIME 邮件的标准；

而 RFC 2633 (http://www.ietf.org/rfc/rfc2633.txt) 增强了证书处理的 RFC 2312 规范；RFC 2634 (http://www.ietf.org/rfc/rfc2634.txt)通过向 S/MIME 添加其他服务扩展了总体功能，如安全回执、三层包装和安全标签等。

目前，S/MIME 版本 3 已被广泛接受为邮件安全标准。下列 Microsoft 产品可支持 S/MIME 版本 3。

- ❑ Microsoft Outlook® 2000（应用了 SR-1）及更高版本。
- ❑ Microsoft Outlook Express 5.01 及更高版本。
- ❑ Microsoft Exchange 5.5 及更高版本。

Microsoft Outlook 的电子邮件的安全设置如图 4-3 和图 4-4 所示。

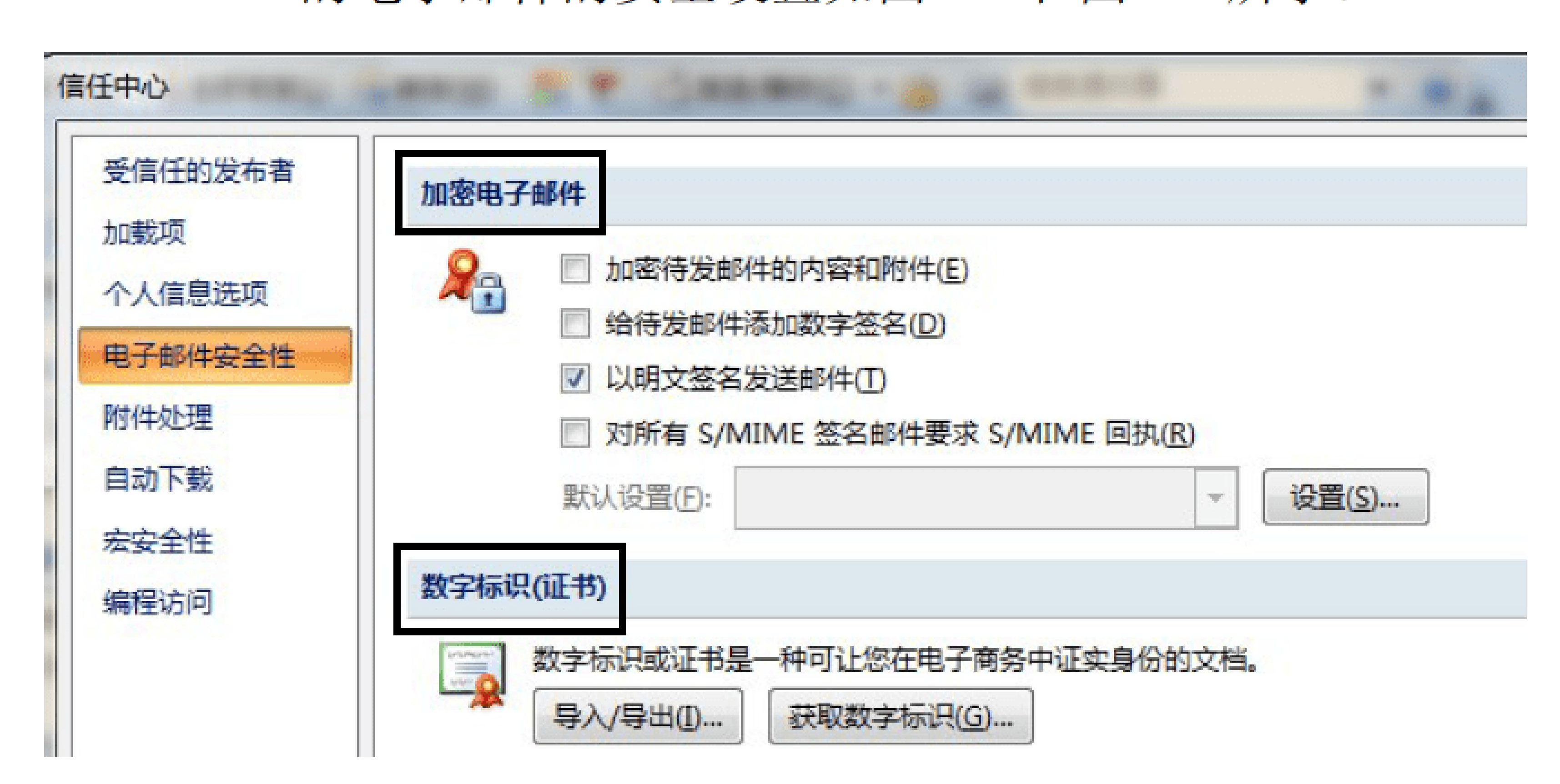


图 4-3　Microsoft Outlook 中的电子邮件安全选项

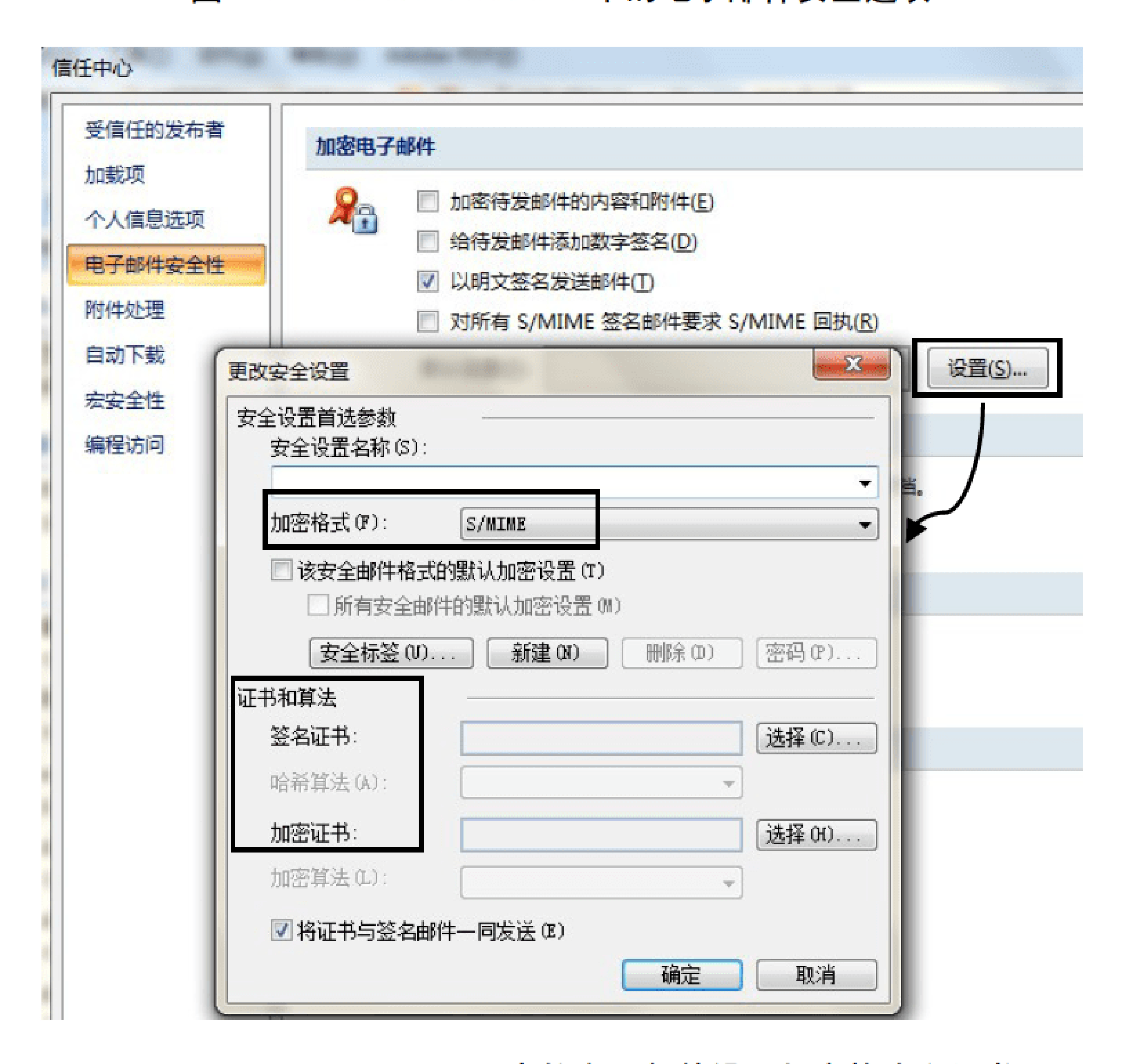


图 4-4　Microsoft Outlook 中的电子邮件设置加密格式和证书

2. S/MIME 的功能

S/MIME 提供两种安全服务——邮件加密和数字签名，即通过加密来保护电子邮件的内容，使用数字签名来验证电子邮件发件人的身份。

邮件加密和数字签名是基于 S/MIME 的邮件安全的核心，与邮件安全有关的其他所有概念都支持这两种服务。在整个邮件安全领域，可能看上去很复杂，但是这两种服务却是邮件安全的基础。

邮件加密和数字签名的实现都是依靠公钥基础设施（PKI）的。通过 PKI 颁发证书，使用证书通过目录访问，实现邮件加密和数字证书。PKI 主要利用了公钥加密，简化了密钥的管理。公钥加密中用到了两种加密：① 对称加密（加密和解密用的是同一把钥匙）；② 非对称加密，加密和解密用的是一对密钥，一个称为公钥，另一个称为私钥，私钥是保密的，它只能由一方保存，公钥是公开的，它可以广泛共享。密钥对在加密和解密过程中相互配合使用，且每个密钥都只能与密钥对中的另一个密钥配合使用。

在邮件收发过程中，因为收发双方是基于特定的操作而需要另一方的公钥或私钥，如发件人用收件人的公钥对电子邮件进行加密，那么电子邮件接收方必须用自己的私钥对邮件进行解密；发件人用自己的私钥对电子邮进行数字签名，那么电子邮件接收方必须用发件人的公钥进行解密，二者关系分别见表 4-1。

表 4-1 电子邮件收发双方的关系

	发件人持有	收件人持有
邮件加密	收件人公钥	收件人私钥
数字签名	发件人私钥	发件人公钥

S/MIME 中，邮件加密和数字签名这两项服务的实现原理如下。

（1）邮件加密

邮件加密提供了针对信息泄露的解决方案。电子邮件有可能在传送的过程中或存储的位置泄露其内容， S/MIME 拥有保密性和数据完整性这两项安全服务，它通过加密的方式来解决这些问题。电子邮件实现加密的原理如图 4-5 所示。

（2）邮件数字签名

数字签名就像是具有法律意义的传统签名的数字化形式。S/MIME 的数字签名提供的安全服务功能有身份验证、认可性和数据完整性。实现电子邮件数字签名的原理如图 4-6 所示。

4.2.2 Web 安全

1. HTTPS

Netscape 公司提出了 SSL 的服务来增加应用层协议中的保密性，完整性与可靠性，其主要用于提升 Web 客户机与服务器之间的安全性。Web 浏览器普遍将 HTTP 和 SSL

相结合，从而实现安全通信，可以看到，使用了 SSL 的 Web 站点前缀为 https://，这个是 HTTP 与 SSL 结合后的缩写。 SSL 后来演变成 TLS 标准，在 RFC2246 中对其有详细的介绍。

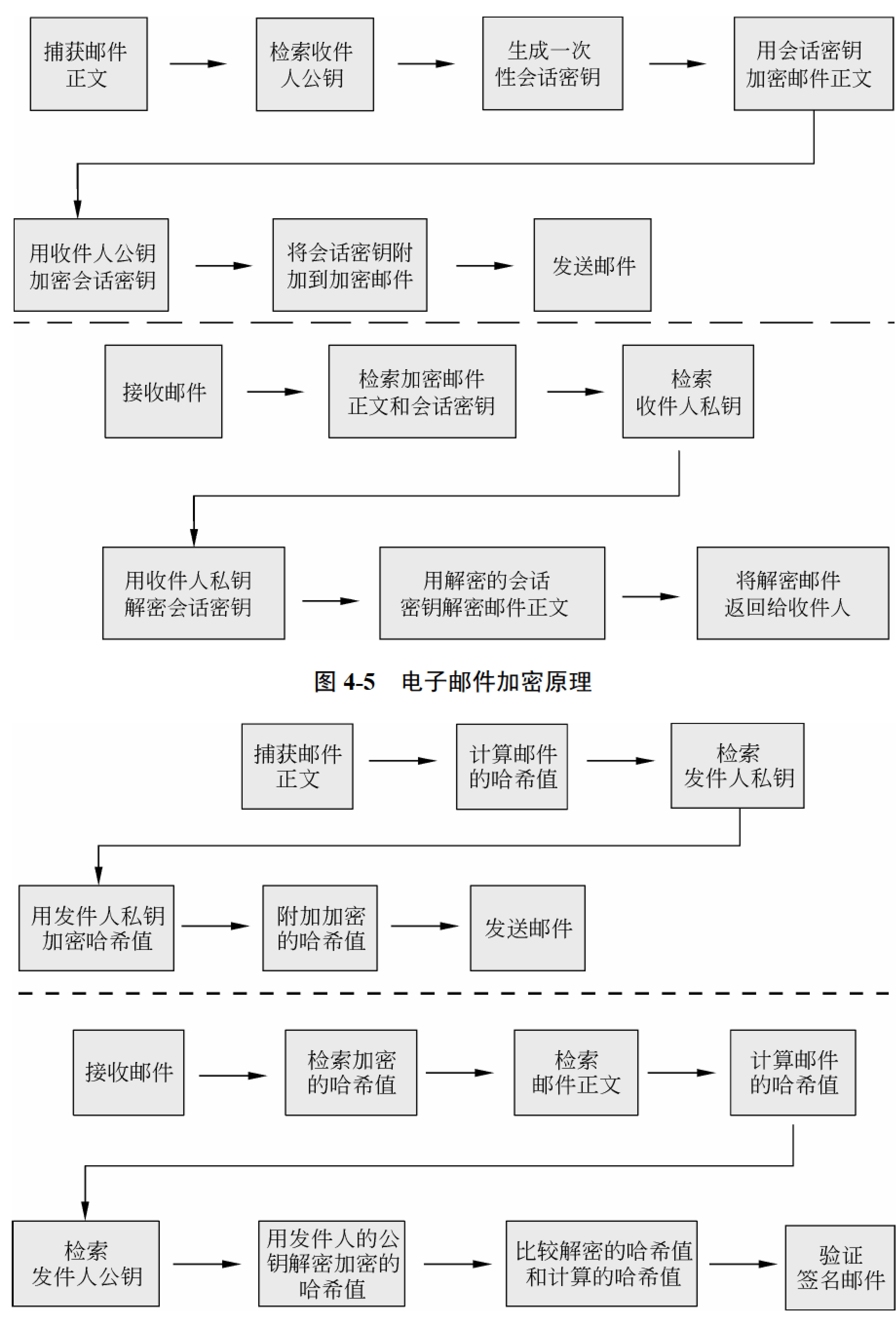


图 4-5　电子邮件加密原理

图 4-6　电子邮件数字签名原理

SSL 是用于解决系统之间数字证书传输问题的，在通信开始时，服务器必须先给客户端发送一个数字证书来提供公钥并认证其身份，当客户端认可了证书的真实性后，双

方才会通过解密数据进行通信。有时，SSL 也会允许进行双向认证。

2. HTTP-S

与 SSL 一样，HTTP-S 也为 Web 服务提供保密性，完整性和可靠性的安全服务，两者的不同主要表现以下几个方面。

（1）SSL 是一个面向连接的协议（用于为两个实体之间提供认证、数据的保密性和完整性服务），而 HTTP-S 是一个面向无连接的协议。

（2）HTTP-S 为 HTTP 客户机和服务器提供多种安全机制，适用于各类潜在的用户。

（3）SSL 工作在会话层和传输层，而 HTTP-S 工作在应用层。

在描述 Web 安全方面，术语的使用是有些容易让人混淆的，HTTP 站点加入 SSL 以后，缩写改为“https”，而 secure-HTTP 也缩写为 HTTP-S。

4.2.3 SET

电子商务在给商家和消费者提供机遇和便利的同时，也面临着巨大的挑战，即交易的安全问题。在电子交易的环境中，消费者希望在交易中保密自己的账户信息而被人窃取；网上商家则希望客户的定单不可抵赖，并且，在交易过程中，交易各方都希望验明对方的身份，以防止上当受骗。

为了实现更加完善的即时电子支付，SET 协议（Secure Electronic Transaction，安全电子交易协议）应运而生。SET 是由 Visa、Microsoft、IBM、RSA、Netscape、MasterCard 等公司开发出的加密协议。SET 协议非常复杂，描述了交易各方之间的关系，它对信息格式、加密方式、交易流程等进行了详尽的定义。SET 不仅是一个技术协议，而且还规定了各方的数字证书的含义、响应动作以及与交易相关的责任认定。SET 协议是 B2C 上基于信用卡支付模式而设计的，保证了开放网络上使用信用卡进行网上购物的安全，它具有的保证交易数据的完整性、交易的不可抵赖性等优点，因此已经成为目前公认的信用卡网上交易的国际标准。在每一次交易中，SET 提供了 4 种服务：可靠性、保密性、信息完整性和可控性。

- **可靠性** 指在交易过程中确保每一方身份的正确性，包括客户、商人、银行等。采用公钥密码体制和 X.509 数字证书标准。
- **保密性** 指使用 DES 加密所有的交易过程，防止入侵者得到交易过程中的任何数据。
- **完整性** 在加密信息里加入消息摘要，防止任何形式的更改。
- **可控性** 允许交易买方在不知道附件内容的情况下也能够验证附件的正确性，这对保护内容保密性起到了重要作用。

1. SET 协议的主要目标和提供的服务

SET 协议的主要目如下。

（1）防止交易信息、账户信息等被非法用户窃取，保证信息在互联网上传输的安全性。

（2）使用了一种双签名技术保证电子商务参与者信息的相互隔离。客户的资料加密后通过商家到达银行，但是商家不能看到客户的账户与密码信息。

（3）解决多方认证问题。不仅对消费者的信用卡认证，而且要对在线商家认证，实现消费者、商家和银行间的相互认证。

（4）保证网上交易的实时性，使所有的支付过程都是在线实时的。

（5）提供一个开放式的标准，规范协议和消息格式，促使不同厂家开发的软件具有兼容性和互操作功能。可在不同的软硬件平台上执行并被全球广泛接受。

SET 提供的服务如下。

SET 协议为电子交易提供了许多保证安全的措施。它能保证电子交易的机密性、数据完整性、交易行为的不可否认性和身份的合法性。SET 协议设计的证书中包括银行证书及发卡机构证书、支付网关证书和商家证书。

（1）保证客户交易信息的保密性和完整性

SET 协议采用了双重签名技术对 SET 交易过程中消费者的支付信息和订单信息分别签名，使得商家看不到支付信息，只能接收用户的订单信息；而金融机构看不到交易内容，只能接收到用户支付信息和账户信息，从而充分保证了消费者账户和定购信息的安全性。

（2）确保商家和客户交易行为的不可否认性

SET 协议的重点就是确保商家和客户的身份认证和交易行为的不可否认性。其理论基础就是不可否认机制，采用的核心技术包括 X.509 数字证书标准、数字签名、报文摘要、双重签名等技术。

（3）确保商家和客户的合法性

SET 协议使用数字证书对交易各方的合法性进行验证。通过数字证书的验证，可以确保交易中的商家和客户都是合法的、可信赖的。

2．SET 协议的购物流程实例

SET 交易过程中要对商家、客户、支付网关等交易各方进行身份认证，因此它的交易过程相对复杂，如图 4-7 所示。

（1）持卡客户在网上商家看中商品后，和商家进行协商，然后发出请求购买信息。

（2）商家要求客户用电子银行付款。

（3）电子银行提示客户输入密码后与商家交换握手信息，确认商家和客户两端均合法。

（4）客户的电子银行形成一个包含订购信息与支付指令的报文发送给商家。

（5）商家将含有客户支付指令的信息发送给支付网关。

（6）支付网关在确认客户信用卡信息之后，向商家发送一个授权响应的报文。

（7）商家向客户的电子银行发送一个确认信息。

（8）将款项从客户账号转到商家账号，然后向顾客送货，交易结束。

从上面的交易流程可以看出，SET 交易过程十分复杂性，在完成一次 SET 协议交易过程中，需验证电子证书 9 次，验证数字签名 6 次，传递证书 7 次，进行签名 5 次，4 次对称加密和非对称加密。根据不同地方的网络设施情况，通常完成一个 SET 协议交易过程大约要花费几分钟甚至更长时间。

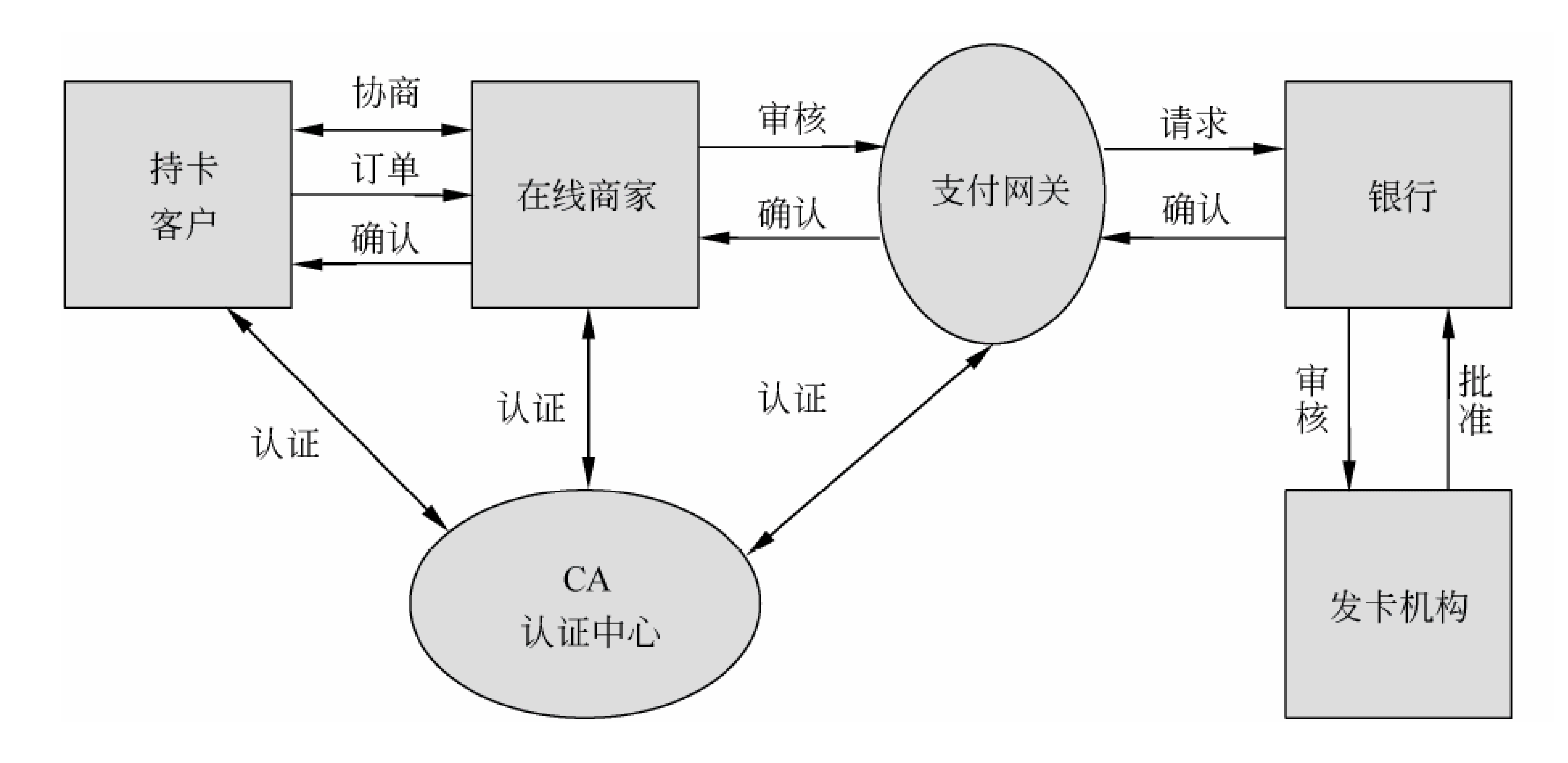


图 4-7　SET 的购物流程实例图

4.2.4　传输层安全

传输层安全（TLS，Transport Layer Security）是 IETF 将提升 Web 站点的安全方法进行标准化的结果，在 RFC2236 中进行了详细的介绍，负责保护应用程序通信过程中传输层的安全性和数据完整性。实际上 TLS1.0 是从 SSL3.0 中演变而来的。目前，最新版本是 RFC 5246，版本 1.2。从技术上讲，TLS1.0 与 SSL3.0 的差异非常微小。

与 SSL 相比，TLS 做了以下改进。

- **互操作性**　一方在不知道对方 TLS 设备细节的情况下，也可以自由的进行 TLS 的参数交换。
- **可扩展性**　可以方便地扩展和调整新的协议。

TLS 利用密钥算法在互联网上提供端点身份认证与通信保密，其基础是公钥基础设施（PKI）。目前，典型的例子中，只有网络服务者被可靠身份验证，而其客户端则不一定。这是由于公钥基础设施普遍由商业运营，且数字签名证书相当昂贵，普通用户很难支付得起证书。TLS 协议的设计在某种程度上能够使主从式架构应用程序通信本身预防窃听、干扰、和消息伪造，它包含 3 个基本阶段。

（1）对等协商支援的密钥算法。

（2）基于非对称密钥的信息传输加密和身份认证、基于 PKI 证书的身份认证。

（3）基于对称密钥的数据传输保密。

TLS 协议包括两个协议组：TLS 记录协议和 TLS 握手协议，每组具有很多不同格式的信息。

（1）TLS 记录协议

TLS 记录协议是一种分层协议，每一层中的信息可能包含长度、描述和内容等字段。它提供的连接安全性具有两个基本特性。

- **私有**　对称加密算法用以数据加密（如 DES 、RC4 等）。对称加密所产生的密钥对每个连接都是唯一的，且此密钥基于另一个协议（如握手协议）协商。此外，记录协议也可以不进行加密使用。

- **可靠** 信息传输包括使用密钥的 MAC 进行信息完整性检查。安全哈希功能（SHA、MD5 等）用于 MAC 计算。记录协议在没有 MAC 的情况下也能操作，但一般只能用于这种模式，即有另一个协议正在使用记录协议传输协商安全参数。

TLS 记录协议用于封装各种高层协议。作为这种封装协议之一的握手协议允许服务器与客户机在应用程序协议传输和接收其第一个数据字节前彼此之间相互认证，协商加密算法和加密密钥。

（2）TLS 握手协议

TLS 握手协议提供的连接安全具有 3 个基本属性。

- 可以使用非对称的，或公共密钥的密码算法来认证对等方的身份，该认证是可选的。
- 共享加密密钥的协商是安全的，协商加密对偷窃者来说是难以获取的。
- 协商是可靠的。如果没有经过通信方成员的检测，任何攻击者都不能修改通信协商。

TLS 的最大优势就在于：TLS 独立于应用协议，高层协议可以透明地分布在 TLS 协议上面。但是，TLS 标准并没有规定应用程序如何在 TLS 上增加安全性，它把如何启动 TLS 握手协议以及如何解释交换的认证证书的决定权留给协议的设计者和实施者来判断。

4.2.5 虚拟专用网络

虚拟专用网（Virtual Private Network，VPN）指通过公用网络（通常是互联网）建立专用网络实现安全通信目的技术。整个 VPN 网络中任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台上，用户数据在逻辑链路中传输，如图 4-8 所示。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

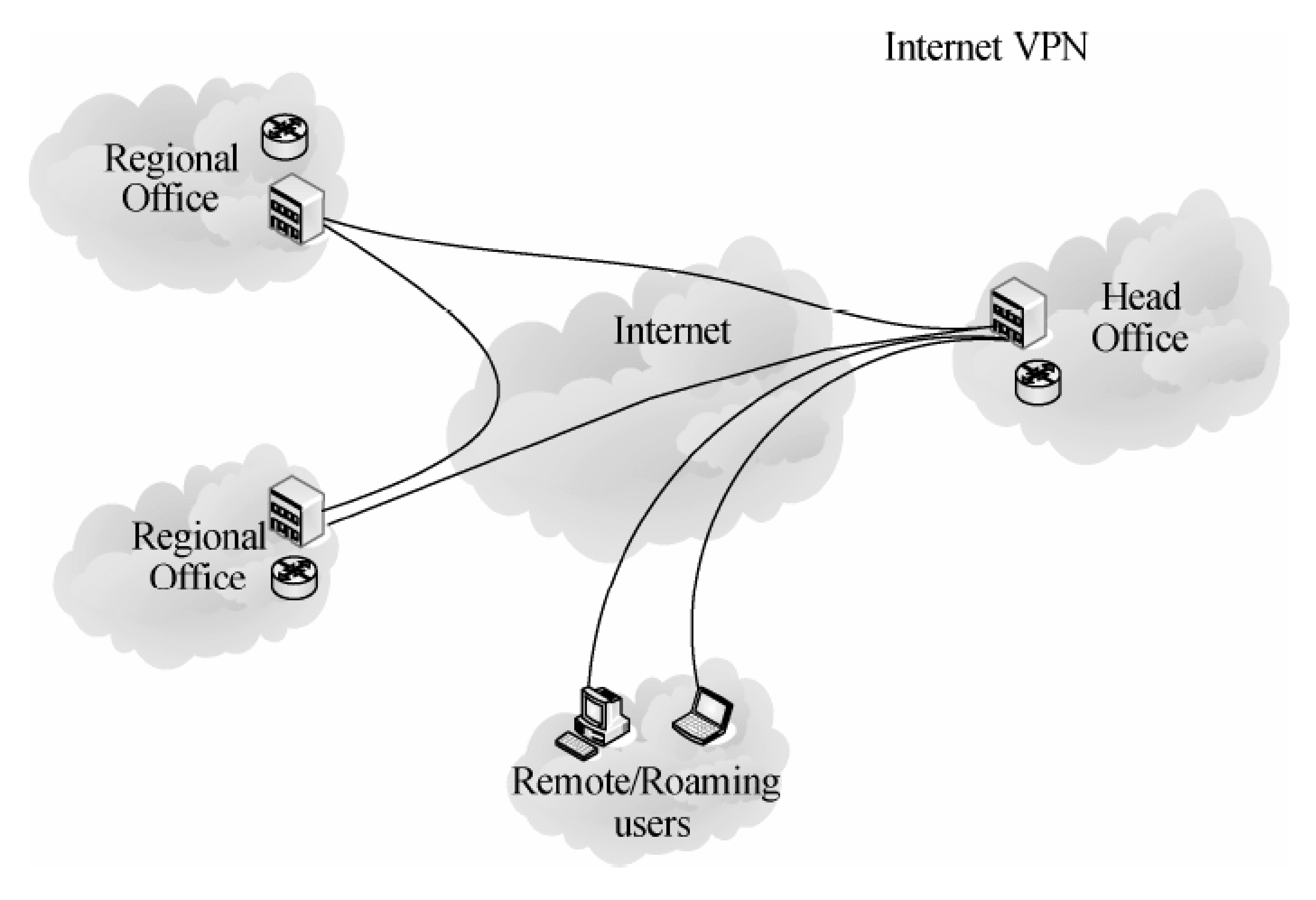


图 4-8 VPN 示意图

例如甲公司内某部门员工张三想要与乙公司某部门员工李四进行通信，张三知道李四工作的具体部门和公司地址，但是李四工作的具体部门信息是不能暴露在公用网络上的，因此张三会将他要寄出的信（信上注明了李四的具体部门）封装在一个大信封里，大信封上的地址是甲公司的地址和乙公司的地址。乙公司收发部门的员工接受到信件后，进行拆封，并将里面的邮件以公司内部邮件方式寄给李四。这种方法的好处是：邮件在两个公司传输过程中只会暴露出两个公司的地址信息，而不会具体暴露张三与李四的具体地址信息。

在网络环境下，路由器充当了收发部门的角色，VPN 的建立可以在路由器端通过加密来有效隐藏通信双方 IP 地址等敏感信息，从而达到在不可信的信道里安全通信的目的。

VPN 主要完成以下工作。

- **IP 加密** 包括把 TCP/IP 的数据包封装在另一个数据包中，然后在报头加入到目的防火墙的路由信息。
- **加密** 对数据包的数据部分进行加密，在传输模式下，数据在生成的时候就被加密，而在隧道模式下，数据内容与数据头都是在传输的过程中被加密和解密的。
- **认证** 认证接收到的数据包的真实性。

VPN 的主要特点如下。

- **安全保障** VPN 通过建立一个隧道，利用加密技术对传输数据进行加密，以保证数据的私有性和安全性。
- **服务质量保证** 根据不同需求，VPN 可以提供不同等级的服务质量保证。
- **可扩充、灵活性高** VPN 支持通过 Internet 和 Extranet 的任何类型的数据流。
- **管理方便** VPN 可以从运营商和用户角度进行方便的管理。

实现 VPN 的主要技术如下。

- **隧道技术** 实现 VPN 的最关键部分是在公网上建立虚信道，而建立虚信道是利用隧道技术实现的，IP 隧道的建立可以是在网络层和数据链路层。
- **隧道协议（Tunneling Protocol）** 隧道是利用一种协议传输另一种协议的技术，即用隧道协议来实现 VPN 功能。为了创建隧道，隧道的服务器和客户机必须使用相同的隧道协议。
- **加解密技术** 加解密技术是目前数据通信中比较成熟的技术，VPN 可直接利用现有加解密算法实现加解密。
- **密匙管理技术** 密匙管理技术的主要功能是如何在公用数据网上安全地传递密匙而不被窃取。
- **使用者与设备身份认证技术** 目前最常用的使用者与设备认证是使用者名称与密码或卡片式认证等方式。

根据不同的划分标准，如 VPN 的协议、VPN 的应用、VPN 所用的设备类型等，可

以对 VPN 进行不同的分类，见表 4-2、表 4-3 和表 4-4。

表 4-2　VPN 按协议分类

按 VPN 的协议划分	描述
PPTP（Point to Point Tunneling Protocol，点对点隧道协议）	一种支持多协议虚拟专用网络的网络技术，是在 PPP 协议的基础上开发的一种新的增强型安全协议，可以通过密码身份验证协议（PAP）、可扩展身份验证协议（EAP）等方法增强安全性。它工作在第二层，可以使远程用户通过拨入 ISP、通过直接连接 Internet 或其他网络安全地访问企业网
L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）	由 IETF 起草，Microsoft、Ascend、Cisco、3COM 等公司参予制定的二层隧道协议，基于 Microsoft 的点对点隧道协议（PPTP）和 Cisco 二层转发协议（L2F）之上，结合了 PPTP 和 L2F 两种二层隧道协议的优点，已经成为 IETF 有关二层通道协议的工业标准。它工作在 OSI 模型的第二层，这种虚拟私有网络可以被因特网服务提供商和企业通过因特网使用
IPSec（Internet 协议安全性）	是一套比较完整成体系的 VPN 技术，它规定了一系列的协议标准，是第三层隧道协议，也是最常见的协议。常见的 IPSec VPN 类型有站到站（site to site）、easy VPN（远程访问 VPN）、DMVPN（动态多点 VPN）、GET VPN（Group Encrypted Transport VPN）等

表 4-3　VPN 按应用分类

按 VPN 的应用划分	描述
Access VPN（远程接入 VPN）	客户端到网关，使用公网作为骨干网在设备之间传输 VPN 的数据流量
Intranet VPN（内联网 VPN）	网关到网关，通过企业的网络架构连接来自相同企业的资源
Extranet VPN（外联网 VPN）	与合作伙伴企业网构成 Extranet，将一个企业与另一个企业的资源进行连接

表 4-4　VPN 按所用的设备类型分类

按 VPN 所用的设备类型划分	描述
路由器式 VPN	路由器式 VPN 部署相对比较容易，只要在路由器上添加 VPN 服务即可
交换机式 VPN	主要应用于连接用户较少的 VPN 网络
防火墙式 VPN	防火墙式 VPN 是最常见的一种 VPN 的实现方式，许多厂商都提供这种配置类型

4.2.6　拨号用户远程认证服务

RADIUS（Remote Authentication Dial In User Service）是一个用于远程用户认证和统计的服务，它包含了 PAP、CHAP。尽管它主要由服务提供商使用，但它也同样可以使用于私有网络集中为所有拨号连接者提供认证和统计服务。例如，很多公司都有很多员工在外地工作，这些员工也许就要使用拨号登入服务了，还有一些厂商或者该公司的合作伙伴为了获取该公司的信息也许要使用拨号登入服务，那么对这些情况进行认证和统计，RADIUS 不失为一个好的工具。

具体来说，RADIUS 有两个主要组件：认证协议和统计协议。

- ❑ **认证协议** 一旦登录到 RADIUS 的服务器，用户就要和自己提供的数据一起接受认证，认证的方式有短时间内回答服务器的问题和使用 PAP，CHAP 协议两种。
- ❑ **统计协议** RADIUS 有 3 种嵌入式统计模式——UNIX 统计模式、详细统计模式、SQL 统计模式。

1. RADIUS 的核心特性

RADIUS 具有如下核心特性。

- ❑ **C/S 结构** 在 C/S 结构中，客户端负责将用户的信息传送给特定的 RADIUS 服务器，然后对反馈的信息进行响应。在另一方面，服务器负责接受客户端发送过来的用户连接请求，验证用户，然后反馈给客户端必要的信息让其决定是否给用户提供服务。
- ❑ **网络安全** 客户端与 RADIUS 服务器之间的所有通信都是通过一个共享密钥进行加密的，当然该密钥对外界是保密的。
- ❑ **灵活的认证机制** RADIUS 服务器可以通过不同的方法对用户进行验证，例如 PPP、PAP 或 CHAP 等方法。
- ❑ **可扩展** RADIUS 是一个支持扩展的系统，其支持两种可扩展语言：嵌入式重写脉冲和 Scheme 语言。当然根据 RFC2138 的规定，所有的会话都由{属性—长度—值}三元组组成，任何新加入的属性值都不能打乱已存在协议的执行。

2. 标准 RADIUS 协议包结构

标准 RADIUS 协议包结构如图 4-9 所示。

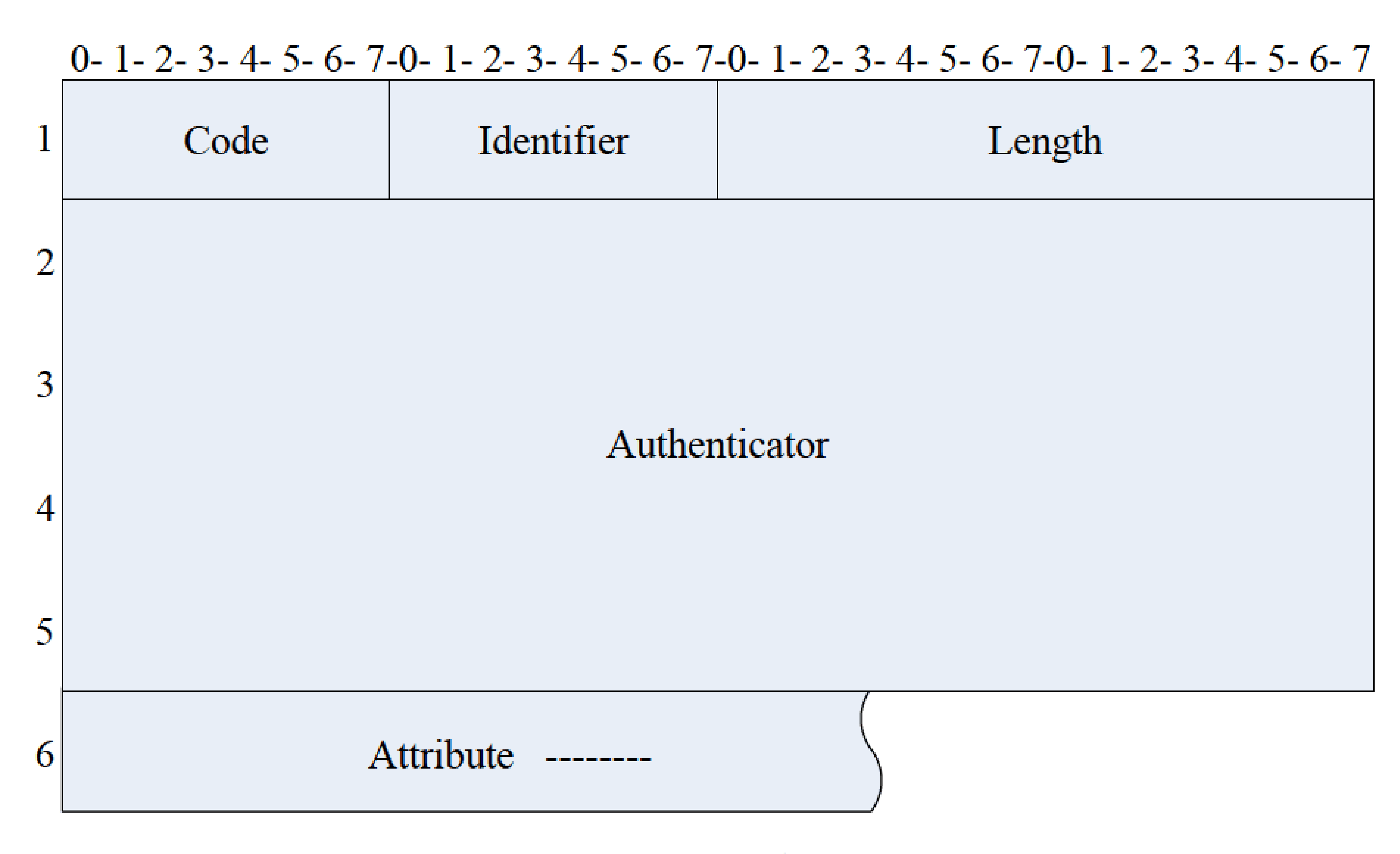


图 4-9 Radius 包格式

Code：包类型，1 字节，指示 Radius 包的类型。表 4-5 中列出了 Code 字段定义的值。

表 4-5　Code 字段定义的值

代码（十进制）	数据包
1	Access-Request 请求访问
2	Access-Accept 接受访问
3	Access-Reject 拒绝访问
4	Accounting-Request 计费请求
5	Accounting-Response 计费响应
11	Access-Challenge 挑战访问
12	Status-Server——Experimental 服务器状况（实验）
13	Status-Client——Experimental 客户端状况（实验）
15	Reserved 保留

- **Identifier**　包标识；1 字节，取值范围为 0～255；用于匹配请求包和响应包，同一组请求包和响应包的 Identifier 应相同。
- **Length**　包长度；2 字节；整个包中所有域的长度。
- **Authenticator**　16 字节长；用于识别和验证 RADIUS 服务器传回来的请求以及隐藏口令算法中的答复。该验证字分为两种：Request Authenticator 和 Response Authenticator。

（1）Request Authenticator（请求验证字）用在请求报文中，必须为全局唯一的随机值。在“Access-Request”数据包中，Authenticator 是一个 16 字节的随机数，称为“Request Authenticator”。

（2）Response Authenticator（响应验证字）用在响应报文中，用于鉴别响应报文的合法性。在“Access-Accept”、“Access-Reject”和“Access-Challenge”中的 Authenticator 域被称为“Response Authenticator”。

响应验证字=MD5(Code+ID+Length+请求验证字+Attributes+Key)

Attributes：属性部分中的 RADIUS 消息包含一个或多个 RADIUS 属性，它们用于执行 RADIUS 消息的特定身份验证、授权、信息和配置详细信息，如图 4-10 所示。

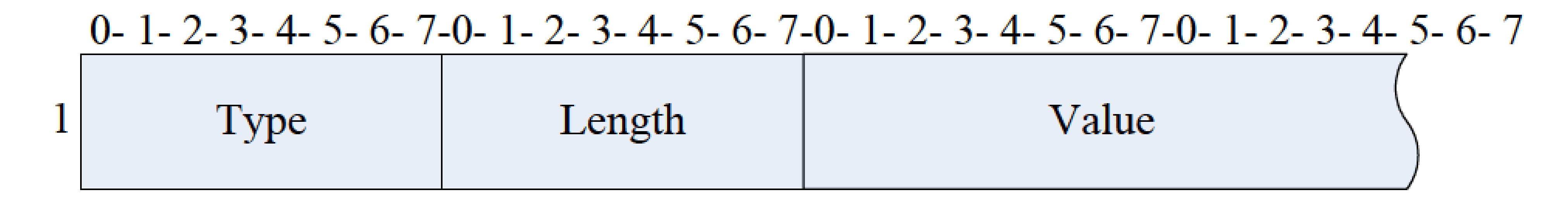


图 4-10　Radius 包结构的 Attributes 部分

3. RADIUS 协议基本交互步骤

RADIUS 协议的基本交互步骤如图 4-11 所示。

（1）用户输入用户名和口令。

（2）RADIUS 客户端根据获取的用户名和口令，向 RADIUS 服务器发送认证请求包（Access-Request）。

（3）RADIUS 服务器将该用户信息与 Users 数据库信息进行对比分析，如果认证成功，则将用户的权限信息以认证响应包（Access-Accept）发送给 RADIUS 客户端；如果

认证失败，则返回 Access-Reject 响应包。

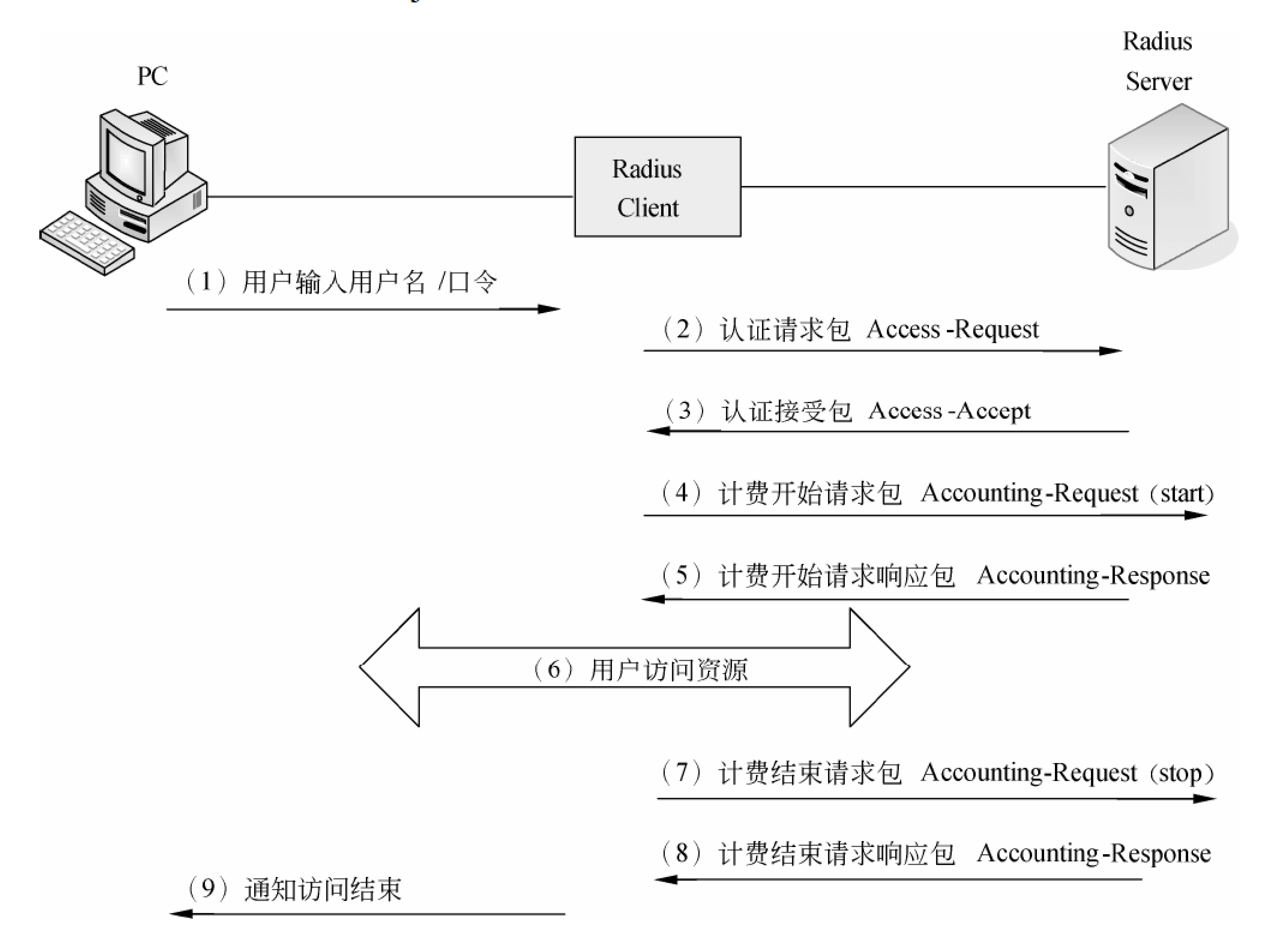


图 4-11　Radius 协议的基本交互过程

（4）RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果可以接入用户，则 RADIUS 客户端向 RADIUS 服务器发送计费开始请求包（Accounting-Request），status-type 取值为 start。

（5）RADIUS 服务器返回计费开始响应包（Accounting-Response）。

（6）RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request），status-type 取值为 stop。

（7）RADIUS 服务器返回计费结束响应包（Accounting-Response）。

4.3 Kerberos

4.3.1 Kerberos 的概念

Kerberos 是由麻省理工学院开发研制的一种计算机网络授权协议，用来在非安全网络中对个人通信以安全的手段进行身份认证。此外，这个词也指麻省理工学院为这个协议开发的一套计算机软件。软件设计上采用 PKI 技术和客户端/服务器结构，并且能够进行相互认证，即客户端和服务器端均可对对方进行身份认证，可用于防止窃听、防止 replay 攻击、保护数据完整性等场合，是一种应用对称密钥体制进行密钥管理的系统。

Kerberos 的扩展产品也使用公开密钥加密方法进行认证。

Kerberos 认证身份不依赖主机操作系统的认证、不信任主机地址、不要求网络中的主机保持物理上的安全。在整个网络中，除了 Kerberos 服务器外，其他都是危险区域，任何人都可以在网络上读取、修改、插入数据。Kerberos 典型的应用是当用户试图使用一项网络服务的时候，服务器需要保证用户就是所声称的那个人。为了实现这个目的，Kerberos 用户首先获得由 Kerberos 认证服务器（AS）发布的票据许可票据。然后，票据许可服务器（TGS）通过检查此票据来核实用户的身份。审核之后，用户就会获得一个由 TGS 颁发的票据（访问票据/服务允许票据），以此得到服务器的认证，得到对服务的访问权。

4.3.2 Kerberos 服务所要满足的目标

Kerberos 所要满足的安全目标主要有几下几方面。

- **安全性** 要足够安全防止潜在的窃听者窃取信息。
- **高可靠性** 如果有一个其他的服务架构能够完全复制此 Kerberos，那么就说明这个系统是不可信的。
- **透明性** 用户除了输入密码以外感觉不到任何其他事情的发生。
- **可扩展性** 可实时地接受并支持新的客户端，服务器的加入。

为了满足这些要求，Kerberos 被设计成可信的第三方服务器来仲裁客户端与普通服务器之间的认证。

4.3.3 Kerberos 认证过程

Kerberos 使用被称为密钥分发中心（KDC）的“可信赖的第三方”进行认证。密钥分发中心 KDC 由认证服务器 AS（Authenticator Server）和票据授权服务器 TGS（Ticket Granting Server）两部分组成，它们同时连接并维护一个中央数据库存放用户口令、标识等重要信息。整个 Kerberos 系统由 4 部分组成：认证服务器（AS）、票据授权服务器（TGS）、用户 C、服务器 S。

协议的安全主要依赖于参加者对 Kerberos 票据的认证声明。简单地说，用户 C 向 AS 认证时用了一个长期共享秘密，并从 AS 得到一个票据。随后，用户可以使用这个票据得到与服务器 S 通信时必须的附加票据，而不需要使用共享秘密。这些票据可以向 S 证明身份。

图 4-12 给出了用户 C 请求服务 S 的整个 Kerberos 认证的过程。

1. 用户 C 请求票据许可票据

这项工作在用户登录工作站时进行。登录时，用户被要求输入用户名。之后会向 AS 发送一个明文消息，里面包含了用户名和用户所请求的 TGS 服务名称。

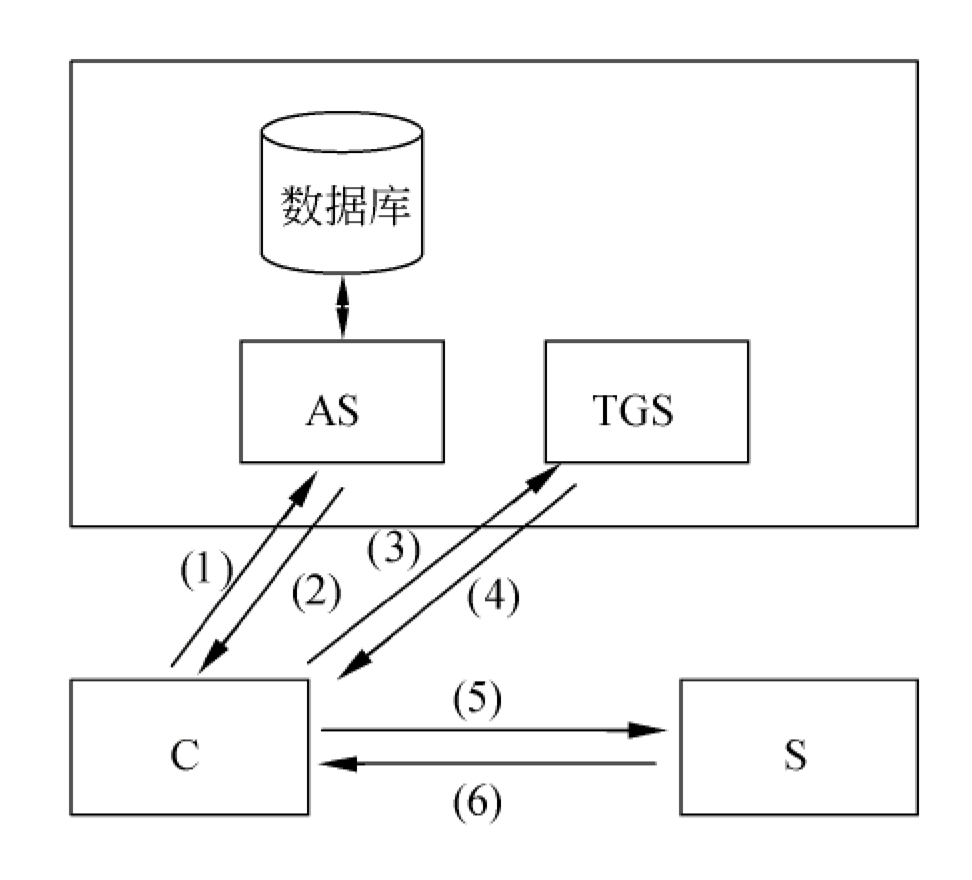


图 4-12　Kerberos 认证过程

2. AS 发放票据许可票据和会话密钥

AS 校验这个用户是否在它的数据库里。如果在，AS 返回以下两条信息给用户。

- **消息 A**　用用户密钥加密的用户/TGS 会话密钥。
- **消息 B**　用 TGS 密钥加密的票据授权票据（包括用户 ID，用户网络地址、票据有效期、客户/TGS 会议密钥）。

用户收到消息 A 和 B，解密消息 A 得到用户/TGS 会话密钥。会话密钥用在将来与 TGS 的通信中（注意：用户不能解密消息 B，因为它是用 TGS 的密钥加密的）。这样的话，用户就拥有足够的信息向 TGS 证明自己的身份。

3. 用户 C 请求服务器票据

用户向 TGS 发送以下两条消息。

- **消息 C**　由从消息 B 中获取的票据授权票据和申请的服务的 ID 组成。
- **消息 D**　用用户/TGS 会议密钥加密的认证（由用户 ID 和时间戳组成）。

4. TGS 发放服务器票据和会话密钥

基于收到的消息 C 和 D，TGS 从消息 C 中重新获取消息 B。它用 TGS 的密钥解密消息 B。这一步使它得到“用户/TGS 会话密钥”。通过使用这个密钥，TGS 解密消息 D（认证），而后返回给用户以下两条信息。

- **消息 E**　用服务器密钥加密的用户/服务器票据（包括用户 ID，用户网络地址，用户/服务器会话密钥的有效期）。
- **消息 F**　用用户/TGS 会议密钥加密的用户/服务器会议密钥。

5. 用户 C 请求服务

基于从 TGS 收到的消息 E 和 F，用户有足够的信息向服务器 S 认证自己。用户联系 S，并向它发出以下两条消息。

- 消息 E　由之前步骤得到（用户/服务器票据，用服务器的密钥加密）。
- 消息 G　用客户/服务会议密钥加密的一个新的认证，包括用户 ID、时间戳。

6. 服务器 S 提供服务器认证信息

S 用自己的密钥解密票据重新得到用户/服务器会话密钥。用这个会话密钥，S 解密得到认证，并返回以下消息给用户，确认他的身份真实，并愿意向用户提供服务。

- 消息 H　在用户认证中找到时间戳加 1，并用用户/服务器会话密钥加密。

用户 C 收到消息 H 后，使用用户/服务器会话密钥解密，并检查时间戳是否被正确更新。如果是，用户可以信赖服务器，至此完成了用户和服务器的双向认证。然后，用户可以向服务器发送服务请求。

4.4 安全套接层 SSL

4.4.1 SSL 的概念

SSL（Secure Sockets Layer 安全套接层）及传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。SSL 与 TLS 在传输层对网络连接进行加密。

SSL 是一个安全协议，提供了 TCP/IP 通信应用程序间的保密性与完整性。通常来讲，SSL 一般用于互联网超文本传输协议（HTTP）。

在 SSL 的实际应用中，客户端与服务器间传输的数据通过使用对称加密算法（如 DES）进行加密，并通过使用公用密钥算法（通常为 RSA）来获得加密密钥交换和数字签名，算法中使用的密钥即服务器 SSL 数字证书中的公用密钥。因为有服务器的 SSL 数字证书，客户端可以验证服务器的身份。在 SSL 协议的版本 1 和 2 中只提供服务器认证。版本 3 添加了客户端认证，此认证同时需要客户端和服务器的数字证书。

4.4.2 SSL 连接

SSL 会话的建立首先是通过 SSL 握手完成的，图 4-13 给出了 SSL 的握手过程。

SSL 连接总是由客户端发起，在会话开始时执行 SSL 握手，此握手最终产生会话的密码。

（1）客户端首先向服务器发送安全会话的请求。

（2）服务器接收到客户端发送的安全会话请求后，会向客户段发送一个 X.509 证书，其中包含了服务器的公共密钥。

（3）客户端接收到证书后，首先对服务器的真实性进行认证。认证结束后，客户端随机生成一个与服务器通信的会话密钥，并用服务器的公钥进行加密，发送给服务器。

（4）服务器接收到加密信息后，利用自己的私钥对其进行解密得到会话密钥，双方会话开始。

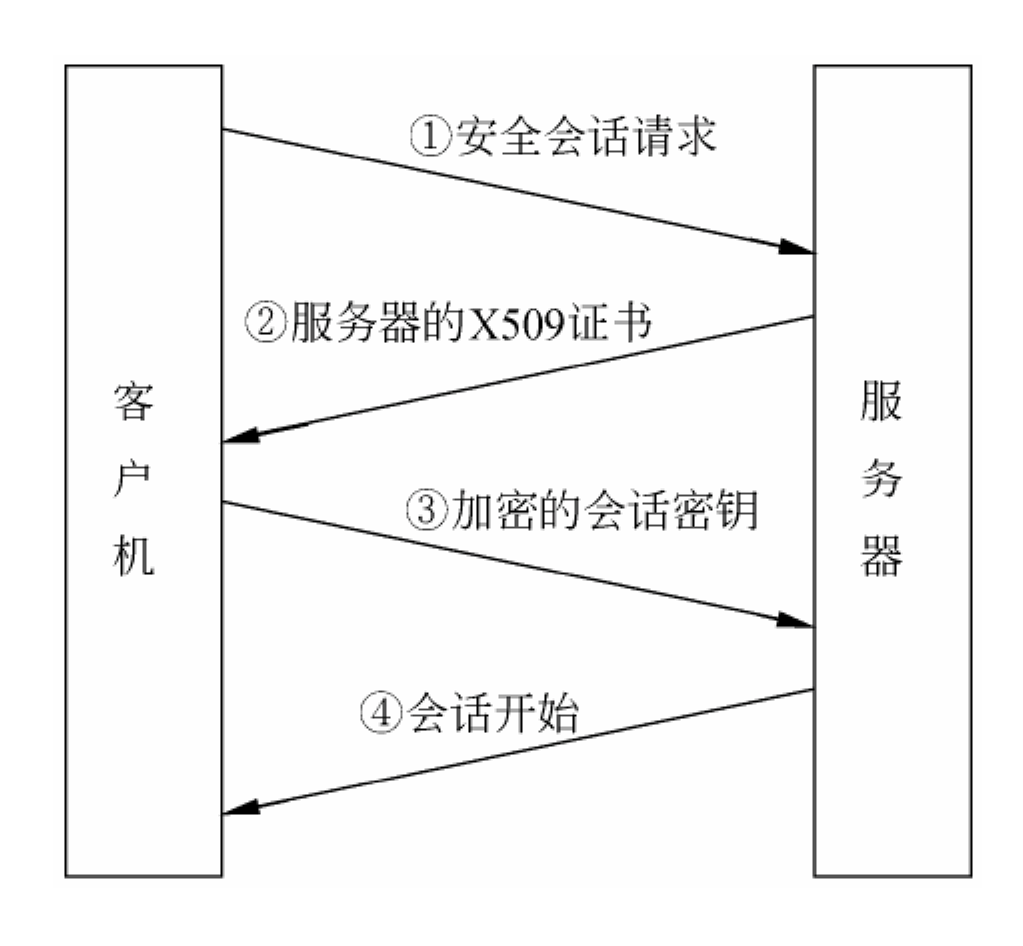


图 4-13　SSL 简单握手

在 SSL V3 中添加了客户端认证服务，因此在第二步的时候，服务器可以对客户端进行认证，服务器会发送“数字证书请求”的消息，其中包含服务器支持的客户端数字证书类型的列表和可接受的 CA 的名称。

对于客户端来说，如果服务器向其请求数字证书，客户端将发送其所持有的数字证书；如果没有合适的数字证书可用，客户端将发送“没有数字证书”的警告。如果需要强制认证客户端数字证书，服务器应用程序将会使会话失败。

4.5 因特网协议安全

因特网协议安全（IPSec）用于增强网络层传输时的安全性，对终端用户是透明的。IPSec 在 IPv4 版本中是可选的，但在 IPv6 版本中是必须安装的。

4.5.1 IPSec 协议分析

IPSec 中有 3 个主要的协议提供安全服务。

- **SA（安全关联）** IPSec 所有的通信都是基于通信系统之间的安全关联 security associations（SAs），这些 SAs 中包含有索引标识和共享密钥所需的基本材料信息。Internet 安全关联和密钥管理协议（ISAKMP）用于在 IPSec 环境中创建并维护这些安全关联。前面提过网路层的 IP 是无连接的，但 SA 的出现，可以让 IPSec 在网络层建立一个逻辑上面向连接的信道，该信道可用于确保发送方的保密性、可靠性、完整性和抗重放攻击。值得注意的是每一个 SA 都只能建立一个单向的信道，所以两方进行通信需要两个 SA。
- **认证头（AH）** AH 增加了报头的信息，并提供了完整性与身份认证。当 AH 用于 IPSec 环境中时，系统通过这种服务可以确定通信角色的真实性。值得注意的是，单独使用 AH 不能提供任何保密性的服务。如图 4-14 所示，认证头（AH）位于 IP 头与数据之间，这样可以有效的保护主机，同时也不影响相邻网络设备的正常工作。

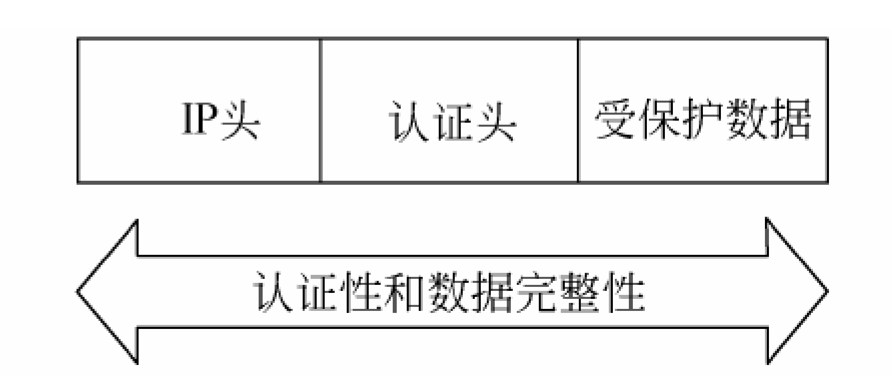


图 4-14　加有 AH 的数据包

- **封装安全载荷（ESP）** 和 AH 一样，ESP 也提供完整性与可靠性，同时也可对数据进行加密以确保数据包的内容不恶意攻击者破获。从图 4-15 可以看出，ESP 对数据包的尾部也进行了封装，这样可以有效的保证载荷的保密性。

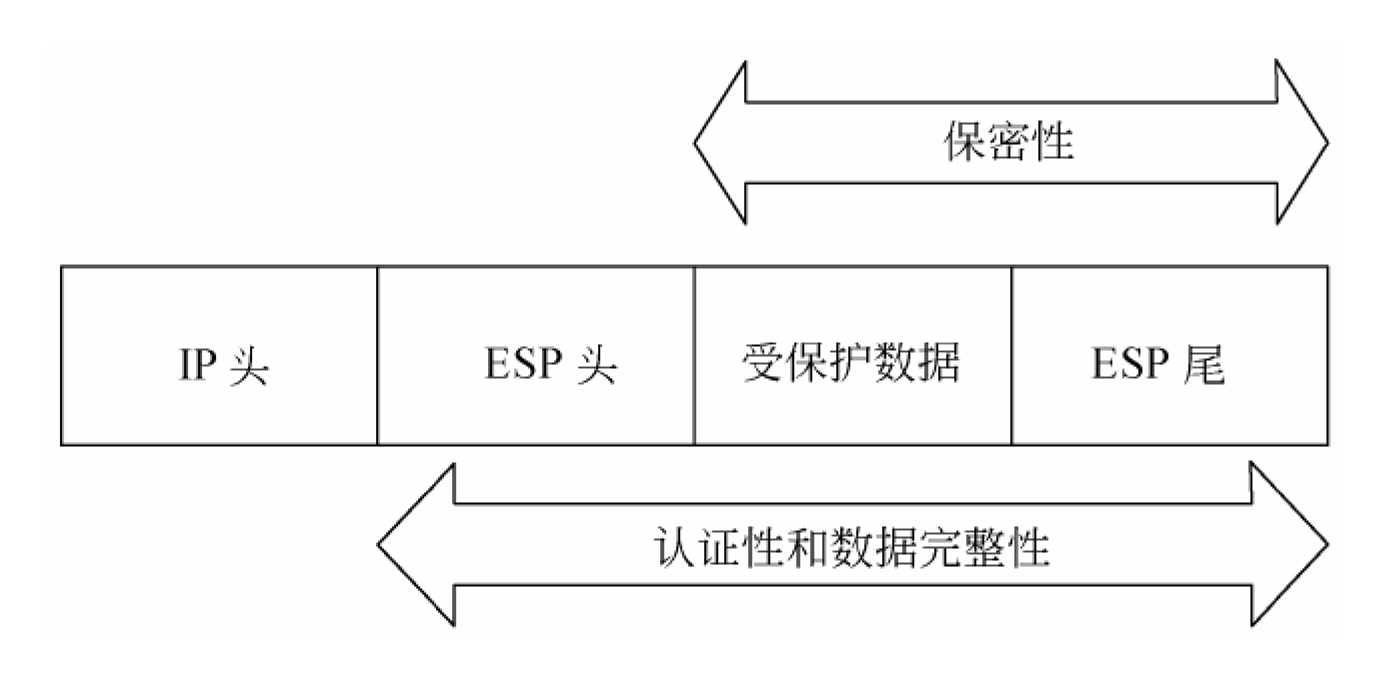


图 4-15　安全封装的数据包

4.5.2　IPSec 加密模式

IPSec 提供两种不同的操作模式，每种模式提供不同的服务，适用于不同的网络环境。

- **传输模式**　此模式用于主机与主机在不支持 IPSec 的网络中通信的情况。在传输模式下，ESP 对数据包的有效载荷提供保密性的安全服务，但数据的首部必须保持非加密状态，只有这样相邻的电脑即使没有 IPSec 的安全关联，也能知道如何处理接收的数据包，否则不能读取地址信息而不能决定数据包下一跳的位置。
- **隧道模式**　在两个网络设备中建立一个虚拟的通道，并对它们之间的所有通信数据进行加密。由于虚拟通道的使用，ESP 可以在隧道模式下加密报文首部，能够有效防止流量分析攻击。所谓流量分析攻击就是恶意攻击方通过监视网络分析网络中的主机正在与谁通信，通信的频率是多少等，挖掘出对自己有用的信息。隧道模式一般用于网关对网关的通信中，例如两个防火墙之间，只有当数据包到达目的网关以后，才会被解密并进行适当的处理。

4.6　点对点协议

早期的互联网用户一般都是通过调制解调器点对点拨号接入互联网的，因此点对点协议（PPP）是一个限制单一数据连接的协议，每一个连接都直接通向远程通道服务器

(RAS)，其作用是认证接入进来的拨号。

PPP 是一种多协议成帧机制，它支持错误检测、选项协商、头部压缩以及使用 HDLC 类型帧格式（可选）的可靠传输。

4.6.1 PPP 的组成

PPP 的组成主要包括以下几部分。

- **封装** PPP 封装提供了不同协议同时在一条链路传输的多路复用技术，能保持对大多数硬件的兼容性。PPP 不仅提供帧定界，而且提供协议标识和位级完整性检查服务。
- **链路控制协议（LCP）** 一种扩展链路控制协议，用于建立、配置、测试和管理数据链路层连接。
- **网络控制协议（NCP）** 协商该数据链路层上所传输的数据包格式与类型，建立、配置不同的网络层协议。

4.6.2 PPP 工作流程

PPP 的工作流程如下。

（1）当用户拨号接入 ISP 时，路由器的调制解调器对拨号做出确认，并建立一条物理连接。

（2）PC 向路由器发送一系列的数据链路层协议（LCP）分组。这些分组及其响应选择一些 PPP 参数，建立数据链路层。之后，PPP 进行网络层配置，网络控制协议（NCP）给新接入的 PC 分配一个临时的 IP 地址，使 PC 成为因特网上的一个主机。

（3）通信完毕时，NCP 释放网络层连接，收回原来分配出去的 IP 地址。

（4）LCP 释放数据链路层连接，最后释放物理层的连接。

上述过程可用图 4-16 所示的状态图来描述。PPP 链路的起始和终止状态是图中的“链路静止”（Link Dead）状态，此时在用户主机和 ISP 的路由器之间并不存在物理层的连接。当用户主机通过调制解调器呼叫路由器时，路由器检测到调制解调器发出的载波信号，双方建立物理层连接。

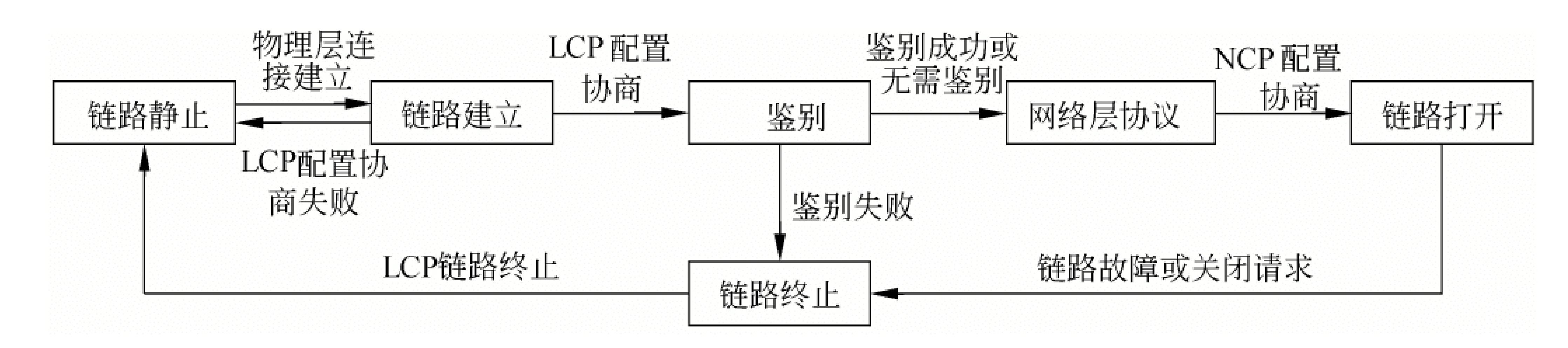


图 4-16 PPP 工作流程

之后，PPP 进入“链路建立”（Link Establish）状态，建立链路层的 LCP 连接。这时，LCP 开始协商一些配置选项，即发送 LCP 的配置请求帧。协商结束后双方就建立了

LCP 链路，接下来进入“认证”(Authenticate)状态。在这一状态，只允许传送 LCP 协议的分组、认证协议的分组以及监测链路质量的分组。可以使用的认证协议包括口令认证协议(PAP)和挑战应答认证协议(CHAP)。若身份认证失败，则转道“链路终止”(Link Terminate)状态。若认证成功，则进入“网络层协议”(Network-Layer Protocol)状态。

在“网络层协议”状态，PPP 链路两端的网路控制协议 NCP 根据不同的协议互相交换网络层特定的网络控制分组。网络层配置结束后，链路进入数据通信的“链路打开”(Link Open)状态。此时，链路的两个 PPP 端点可以彼此向对方发送分组。

数据传输结束后，可以由链路的一端发送终止请求 LCP 分组请求停止链路连接，在接到对方的终止确认 LCP 分组后，转到“链路终止”状态。如果链路出现故障，也会从“链路打开”状态转到“链路终止”状态。当调制解调器的载波停止后，则回到“链路静止”状态。

4.6.3 PPP 认证

对于 PPP，有几种认证协议可被使用，其中有 PAP、CHAP、EAP。

- **密码认证协议（PAP）** 要求申请人重复给服务器发送认证请求信息，包括用户姓名和密码，直到申请人接受到响应或者连接中断。
- **挑战握手认证协议（CHAP）** 其工作在共享密钥的基础上。认证过程为：服务器首先给客户端发送一个挑战信息然后等待客户端的响应；客户端一旦受到挑战信息，会增加一个随机秘密信息，然后将两个信息加在一起求出 hash 值，然后将 hash 值与秘密信息一并发送给服务器；服务器收到客户端发来的信息后也用事先商量好的 hash 函数对两个信息之和求 hash 函数，然后对两者进行比较。服务器会周期性对客户端进行认证。
- **扩展认证协议（EAP）** EAP 是一个开放终端，允许远程 VPN 客户端和验证程序之间进行开端对话。对话由对身份验证信息的验证程序请求和远程 VPN 客户端的响应组成。例如，当 EAP 与安全标记卡一起使用时，验证程序可以单独查询远程访问客户端的名称、PIN 和卡标记值。经过提问和回答一轮查询之后，远程访问客户端将通过身份验证的另一个级别。正确回答所有问题之后，将对远程访问客户端进行身份验证。

协商过程中，客户端和服务器端必须在加密算法和密钥上保持一致，IETF 建议了两种加密算法——DES 和 3DES。

习　　题

一、选择题

1. 在 TCP/IP 协议安全中，下列哪一项属于应用层安全？（　　）
   A. VPNs
   B. PPP
   C. Kerberos
   D. SSL
2. IPSec 中有 3 个主要的协议用来对传输中的系统提供安全服务，不包括下列哪一

项？（　　）

A. SA
B. AH
C. CA
D. ESP

二、简答题

1. 简述SSL的握手过程。
2. IPSec 如何对传输中的系统提供安全服务？
3. 简述电子邮件加密原理。
4. 简述电子邮件数字证书原理。
5. PPP协议是如何工作的？
6. Kerberos的认证过程是如何进行的？
7. Radius协议是如何进行交互的？
8. 简述SET协议购物流程的步骤。
9. VPN是如何工作的？

课后实践与思考

1. 了解您所在的单位/学校的VPN架设情况，并分析其工作原理及分类。
2. 了解您所使用的邮件系统都涉及哪些安全协议。

第 5 章　安全事件处理

本章学习重点：

- 识别并处理系统中的安全事件
- 熟悉常见的攻击方法
- 理解无线网络安全
- 理解传感网络安全

系统安全首要的目标就是维护系统中数据的安全。为了给数据提供高效率的安全保护，必须理解系统中存在的威胁。总的来说，威胁分为自然威胁和人为威胁。对于系统管理员，更应关注如何将人为威胁造成的损失最小化，能够对实时攻击进行识别并做出合理的响应。

本章介绍了几种常见的攻击方式，并说明了当攻击发生时如何分辨，如何响应。对于安全策略来说，第一步就是辨别正在发生的攻击，然后就必须有一个能够处理攻击的计划，计划中必须包括如何对攻击进行响应，对攻击后造成的损失进行恢复等一系列的动作进行详细的规划。

随着互联网技术的发展，无线网络和传感网络的应用日益广泛，如何有效保护无线网络和传感网络的安全正在成为新的研究重点。

5.1 攻击及其相关概念

攻击是指在未授权的情况下访问系统资源或阻止授权用户正常访问系统资源。一个试图进行以上行为的动作就可以被称做攻击，而不是只有成功达到目的的动作才能称做攻击。攻击通过泄密、篡改、毁坏等手段来损坏数据的保密性、完整性、可用性。

- ❑ **攻击者**　指实施攻击行为的主体，可以是一个个体，也可以是一个团体。当攻击实施的时候，攻击者可以使用不同方法，从不同地方同时对目标进行攻击。如果攻击结果违反了法律法规，就可以称之为计算机犯罪。
- ❑ **攻击的类型**　攻击的分类多种多样，根据目的的不同，攻击行为又可以分为军事情报攻击，商业金融攻击，恐怖袭击，基于报复的攻击，以炫耀为目的的攻击。

5.1.1　安全事件

在理解安全事件前，首先要明白攻击与安全事件之间的关联与不同。任何违背本系统安全策略的行为都可以称为安全事件，因此每个攻击都可以视为安全事件，但并不是所有的安全事件都是攻击行为。例如，系统中的口令策略指定不能以词典中可以查到的词作为系统口令，因此如果用户使用 test 作为密码，就可视为安全事件。

安全事件处理最重要的步骤就是能够及时发现已经发生的安全事件。系统管理员必须对系统的安全策略有足够的了解，能在第一时间内知道系统正在遭受的攻击。例如，交警只有对公路上的最高限速有所了解，才能准确判断公路上的汽车是否超速。

当意识到系统存在攻击行为时，就应该迅速寻找到攻击位置并判断攻击类型，通常可以通过对系统日志进行分析得到这些结果。例如，判断对安全文件的非授权访问，最常见的做法就是分析系统权限日志，如果有人越过访问控制机制对安全文件进行了非授权的访问，那么通过日志就可以判断是谁接触过安全文件。当然这种方法也不是绝对有效的，攻击者也可能通过授权用户的账号来请求资源，这样日志中只会记录合法用户的账户。

5.1.2 安全事件类型

以下是 4 种类型的安全事件，这 4 种安全事件都是很常见的攻击方式，所以对它们的检测、预防、响应对保护整个系统安全至关重要。

1. 扫描

扫描就是动态地探测系统中开放的端口，通过分析端口对某些数据包的响应来收集网络和主机的情况。通过扫描，可以判断出网络的拓扑结构，主机的操作系统信息以及主机开放的端口号等一系列信息，为攻击行为做准备。因此，扫描虽然不是攻击行为，但对网络进行的恶意扫描的危害还是相当大的。

2. 非授权访问

非授权访问是指越过访问控制机制在未授权的情况下对系统资源进行访问或是非法获得合法用户的访问权限后对系统资源进行访问。在成功进入系统后，攻击者可以根据其意愿随意泄露、更改、摧毁数据。一次成功的非授权访问可以在事后不留任何痕迹，因此很难被检测。处理这种事件的最好方法就是关注系统正常运行时的数据特征，当发现数据特征的异常行为时，就应意识到系统内有此类事件发生。

3. 恶意代码

恶意代码可以是一个程序，一个进程，也可以是其他的可执行文件，共同特征是可以引发对系统资源的非授权修改或其他的非授权行为。病毒是最常见的一种恶意代码，一般嵌入在可执行文件中，引发某些非授权行为；蠕虫与病毒相似，但其是一个独立的程序，不需要宿主，可自我运行；另一种常见恶意代码是木马，表面看起来是一个正常程序，但还隐藏着其他目的，当木马程序被用户运行时，就会显露出真实的目的，例如恶意篡改文件，自我复制并发送等。

4. 拒绝服务

拒绝服务攻击主要用于破坏数据的可用性。正常情况下，当系统收到授权用户的资源使用请求时，就能够给用户提供服务。拒绝服务攻击的目的就是使系统无法正常向授

权用户提供服务。拒绝服务攻击的危害极大，对服务供应商来说尤为明显。例如当用户在一家网络商城购买商品的时候，发现该网络商城的网站无法正常展示商品特性，用户的第一反应就是去他的竞争对手——另外一家网络商城购物。

5.2 安全事件管理方法

系统管理员意识到系统内有安全事件发生时，就必须将安全事件处理计划付诸于行动。整体来看，处理安全事件大致分为以下几步。

（1）检测安全事件是否发生。

（2）控制事件所造成的损害。

（3）将事件与事件造成的损害上报给合适的认证方。

（4）调查事件的起因、来源。

（5）分析搜索到的线索。

（6）采取必要行动避免类似事件发生。

对于单独用户而言以上工作量过于巨大，因此有必要建立一个包含来自于不同部门成员的事件响应小组。部门成员之间协同工作保证高效处理事件，同时最大限度地降低了事件再次发生的可能性。

响应小组通过使用工具及其他办法调查与控制安全事件，每一种类型的事件都需要通过不同的行为来控制损害程度。例如拒绝服务攻击，通过设置防火墙的黑名单就可以降低攻击的强度。如果系统受到过一次攻击，就很有可能遭受第二次攻击。应该对系统控制重新进行考虑，并对每一类安全事件重新制定防御计划。

在对事件进行响应的时候，响应小组需要收集便于以后分析的信息以及可能成为证据的信息。证据可能是一个硬盘、一个软件或其他可以证明攻击者身份的数据。收集证据也有不同的方法，例如日志分析器、硬盘扫描工具、网络行为踪迹查询等。

事件响应小组发现系统内发生攻击时，首先要确定是否违反了法律法规，有些攻击起初看起来并没有违反任何法律法规，但随着数据的收集，才被发现属于网络犯罪。这时再报警，证据就不具有法律效应，甚至系统管理员也可能因为没有及时报警而引起诉讼。所以最好的做法就是当发现攻击有违反法律法规的可能性时就及时报警。

5.2.1 安全事件预防

一个好的安全策略首先应该制订出响应安全事件方案的大体框架。就像前面提到的，每个组织的应急响应小组成员应该由组织内各个部门的成员构成，这样在事件发生时才能妥善处理系统内受到事件影响的各方面事物。

安全策略的制订也必须囊括所有可能会发生的安全事件，并对每个事件给出合适的响应计划。在制订策略并具体构造响应计划的框架时，网络上有些优秀的资源可以利用，图 5-1 列举出部分资源网站。

在对每个可能发生的安全事件制订响应策略时，系统管理员必须按照一定的规则，将责任落实到每一个人身上。首先确认事件发生时，响应小组内的每一个成员能够明白

针对该事件应该具体做什么事情；另外还要对成员进行换位训练，以防遇到成员不全的情况；最后还要对终端用户进行简单的培训，至少应该让用户能够辨别一些常见的安全事件并且明白处理它们的方法。例如，与可疑主机保持距离，并及时上报给安全处理中心。

Resource	Address
Handbook for Computer Security Incident Response Teams	http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf
Computer Security Incident Response Team	http://www.cert.org/csirts/
Responding to Intrusions	http://www.cert.org/security-improvement/modules/m06.html
Forming an Incident Response Team	http://www.auscert.org.au/render.html?it=2252&cid=1920
SANS IESEC Reading Room: Incident Handling	http://www.sans.org/rr/catindex.php?cat_id=27
FIRST: Forum of Incident Response and Security Teams	http://www.first.org

图 5-1　安全策略资源网站

最重要的是，系统管理员不应该在发现犯罪已经发生后才将情况上报给执法部门，首先与当地的执法部门负责人建立良好的合作关系，在上报时能够明确要上报的对象。同样需要与公司和服务商建立良好的合作关系，这样在需要帮助的时候，可以使事件的处理变得更加方便。

5.2.2　安全事件处理标准的制定

在安全响应小组处理安全事件的过程中，要遵循预先设定的流程进行工作。一部分小组成员负责评估损害程度；一部分成员负责将事件告知管理人员并与服务商联系寻求帮助；而另一个成员需要决定是否需要告知警察来协助调查。所有小组成员都使用标准化的事件响应格式处理事件，这些响应格式详细记录每个成员的名字，要做出的动作，以及事件处理过程中的各种信息。这些标准化的格式就是事件报告的基础。

作为一个响应小组，在响应事件时，正确的做法是确认小组内的每一个成员都会遵循事前制定好的步骤，并且保证所有的处理过程专业化，并有一个记录着从开始到结束过程中每一步操作的详细文档。所以制定事件响应流程的标准是很重要的，这样才能让整个小组高效地完成对事件的响应。

在制定流程标准的时候最好与当地的执法部门联系，将与执法部门相关的要求加入到流程标准中，有助于在普通的安全事件扩大成犯罪事件时进行合理有效的责任转交。

5.2.3　对安全事件的事后总结

当对安全事件进行检测、控制、侦查和解决等一系列动作后，就应该整理关于整个

事件的文档，并进行总结。要收集所有关于此次事件的报告，并将其按时间顺序编辑，最后组织整个事件响应小组成员集中审阅事件报告。

小组会议的主要目标是总结小组在事件中的表现，应该评估在本次响应中成功的地方，并尽可能地提出一些中肯的意见，主要包括以下几种：

（1）哪些是做得好的地方。

（2）响应是否及时并且恰当。

（3）哪些方面还可以提升。

（4）应急响应的动作是否顾及了系统的整体安全。

（5）能够采取什么样的措施来降低同类事件再次发生的可能性。

会议对这些问题进行讨论有助于提升小组的工作效率。对好的方面进行加强，对不好的方面进行改进，小组的工作技能与经验会逐步提升，处理安全事件会日益高效与专业。要重视会议中的所有意见，并将合适的意见调整到下一次的应急响应之中。最重要的是，鼓励所有的小组成员学习其他组织出版的关于事件响应的论文，最经济有效的方式就是学习其他人的经验。重视和其他小组的交流，找出其他响应小组做得好的地方和做得不好的地方，学习长处，从短处中汲取经验教训。

5.3 恶意代码

本节介绍了几种常见的恶意代码的类型，并给出相应的处理方法。恶意代码就是引发非授权修改或其他非授权行为的命令集合。恶意代码进入系统的方式有很多种，可以通过网络进行，也可从可移动介质中植入。

虽然恶意代码可以越过系统防护潜入系统，但有很多方式可以检测并完全摧毁它。通过病毒防护软件对所有的文件进行扫描可以发现恶意代码。主要有两种技术用来进行扫描，一种是寻找大小发生变化或访问时间有变化的可执行文件，另一种是将可执行文件与已知的病毒特征模块进行对比，这也是绝大部分病毒扫描器的工作原理。

恶意代码又分为病毒、蠕虫、特洛伊木马、网络控件等几类。

5.3.1 病毒

病毒是最为常见的一种恶意代码，一个病毒就是一个简单的程序，其目的在于寻找其他的程序，通过将自身的复件嵌入到程序的方式来感染其他程序，被感染的程序就叫做病毒宿主，当主程序运行时，病毒代码同样也会运行。病毒需要一个用于感染的宿主，脱离宿主，病毒就不能自我复制。第 10 章将详细地介绍病毒方面的有关知识。

5.3.2 蠕虫

1. 蠕虫的定义及分类

从对计算机造成损害的意义上说，蠕虫也是一种病毒，具有病毒的传播性、隐蔽性、

破坏性等特性。但蠕虫与病毒在某些方面是不同的。蠕虫不需要宿主程序，通过复制自身在互联网环境下进行传播。同时，与病毒主要是破坏计算机内的文件系统不同，蠕虫的传染目标是互联网内的所有计算机。表 5-1 给出了普通病毒与蠕虫病毒的不同。

表 5-1　普通病毒与蠕虫病毒比较

	普通病毒	蠕虫病毒
存在形式	寄存文件	独立程序
传染机制	宿主程序运行	主动攻击
传染目标	本地文件	网络计算机

根据攻击目标不同，可将蠕虫病毒分为两类。一类是针对计算机网络的，利用系统漏洞，主动进行攻击，可以对整个互联网造成瘫痪性的后果。“红色代码”、“尼姆达”等都是这种类型的蠕虫。另一类是针对个人主机的，通过网络（主要是电子邮件，恶意网页形式）进行迅速传播，“爱虫病毒”、“求职信病毒”是这种类型的蠕虫。在这两类中，第一类具有很大的主动攻击性，而且爆发也有一定的突然性，但查杀这种病毒的困难性较低。第二类病毒的传播方式比较复杂和多样，少数利用了微软的应用程序的漏洞，更多的是利用社会工程学对用户进行欺骗和诱使，造成的损失是非常大的，也更难抵御。

2. 蠕虫的基本结构及传播过程

蠕虫的基本程序结构分为 3 种模块：传播模块、隐藏模块和目的功能模块。传播模块负责蠕虫的传播。隐藏模块负责在蠕虫侵入主机后，隐藏蠕虫程序，防止被用户发现。目的功能模块实现对计算机的控制、监视或破坏等功能。其中，传播模块又可以分为 3 个基本模块：扫描模块、攻击模块和复制模块。图 5-2 给出了蠕虫的基本构造。

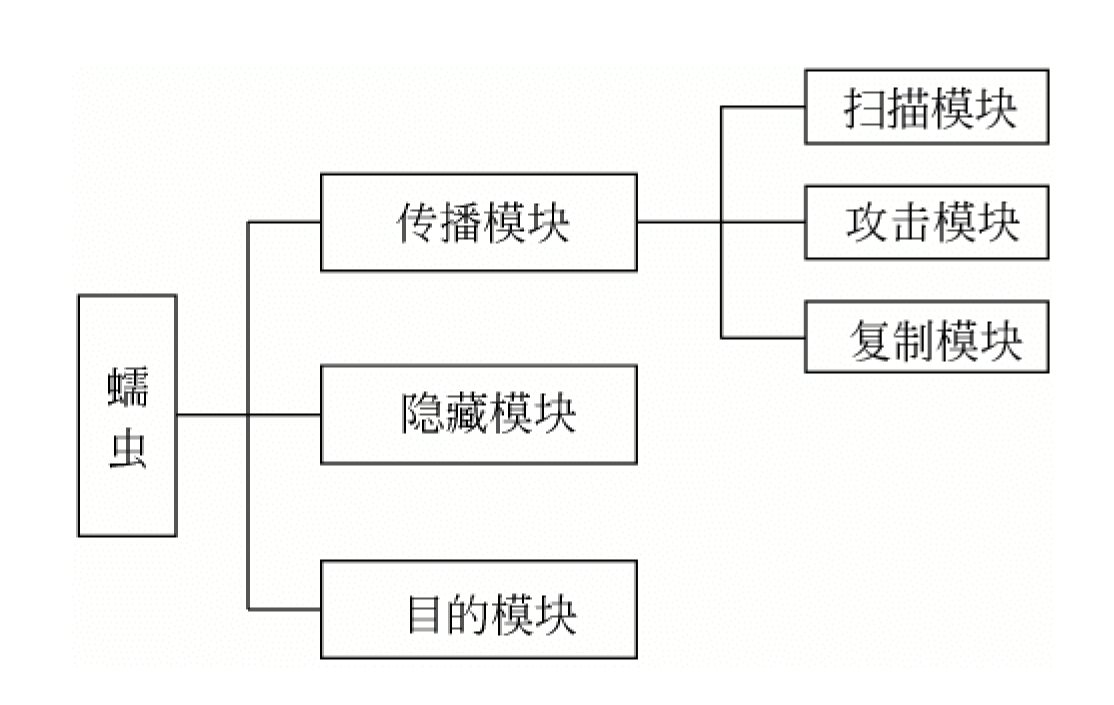


图 5-2　蠕虫的基本构造

蠕虫程序的一般传播过程如下。

- **扫描**　由蠕虫的扫描功能模块负责探测存在漏洞的主机。当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可传播的对象。
- **攻击**　攻击模块按漏洞攻击步骤自动攻击步骤 1 中找到的对象，取得该主机的权限（一般为管理员权限），获得一个 shell。
- **复制**　复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并启动。

3．蠕虫特点及危害

蠕虫的特点主要有几下几方面。

（1）利用操作系统和应用程序的漏洞主动进行攻击。典型的此类蠕虫病毒有“红色代码”和“尼姆达”等。由于 IE 浏览器的漏洞（Iframe Execcomand），感染了“尼姆达”的邮件在不用手工打开附件的情况下就能激活病毒。而“红色代码”是利用了微软 IIS 服务器软件的漏洞（idq.dll 远程缓存区溢出）来传播。

（2）传播方式多样。可利用文件、电子邮件、Web 服务器、网络共享等途径进行传播。

（3）制作技术与传统的病毒不同。利用当前最新的编程语言与编程技术实现，易于修改以产生新的变种，从而逃避反病毒软件的搜索。

（4）与黑客技术相结合，潜在的威胁和损失更大。以红色代码为例，感染后的机器的 web 目录的\scripts 下将生成一个 root.exe，可以远程执行任何命令，从而使黑客能够再次进入主机。

从 1988 年第一个蠕虫病毒产生开始，在二十几年的时间里，蠕虫病毒已经造成了巨大的经济损失。表 5-2 给出了近些年蠕虫所造成的巨大损失。

表 5-2　蠕虫事件及其损失

病毒名称	持续时间	造成损失
莫里斯蠕虫	1988 年	6000 多台计算机停机，直接经济损失达 9600 万美元
美丽杀手	1999 年	政府部门和一些大公司紧急关闭了网络服务器，经济损失超过 12 亿美元
爱虫病毒	2000 年 5 月至今	众多用户电脑被感染，损失超过 100 亿美元以上
红色代码	2001 年 7 月	网络瘫痪，直接经济损失超过 26 亿美元
求职信	2001 年 12 月至今	大量病毒邮件堵塞服务器，损失达数百亿美元
SQL 蠕虫王	2003 年 1 月	网络大面积瘫痪，银行自动提款机运作中断，直接经济损失超过 26 亿美元

5.3.3　特洛伊木马

“特洛伊木马”（简称“木马”）是一种秘密潜伏的能够通过远程网络进行控制的恶意程序。控制者可以控制被秘密植入木马的计算机的一切动作和资源，是恶意攻击者进行窃取信息等的工具。特洛伊木马没有复制能力，它的特点是伪装成一个实用工具或一个可爱的游戏，诱使用户将其安装在 PC 或者服务器上。

“特洛伊木马”一词来源于希腊神话“木马屠城记”。古希腊有大军围攻特洛伊城，久攻不下。于是有人献计制造一只高二丈的大木马，让士兵藏匿于其中，大部队假装撤退而将木马弃于特洛伊城下。城中得知解围的消息后，将“木马”作为战利品拖入城内。午夜时分，匿于木马中的将士开秘门而出，开启城门，和大部队里应外合取得了战争的胜利。后世称这只大木马为“特洛伊木马”。如今黑客程序借用其名，有“一经潜入，后患无穷”之意。

1. 木马组成及启动

完整的木马程序一般由两个部分组成：一个是服务端（被控制端），一个是客户端（控制端）。攻击者首先将服务端植入目标系统，然后利用控制端控制运行服务端的主机。“中了木马”就是指安装了木马的服务端程序。此时，主机上的各种文件、程序，以及在使用的账号、密码都可以通过伪装的进程发送给控制端。

木马都具有自启动功能，可以避免木马因关机操作而失去作用。自启动实现的方法有很多，可以将木马加入到用户经常执行的程序（例如 explorer.exe）中，当用户执行该程序时，木马自动发生作用。当然，更加普遍的方法是通过修改 Windows 系统文件和注册表达到目的，常用的方法主要有以下几种。

（1）在 Win.ini 中启动：Win.ini 的[windows]字段中有启动命令“load=”和“run=”，一般情况下“=”后面是没有内容的，而攻击者可以把木马程序放在“=”后面。举个例子，如果出现下面情况

```
run=c:\windows\file.exe
load=c:\windows\file.exe
```

则，file.exe 很可能就是木马程序。

（2）在 System.ini 中启动：System.ini 位于 Windows 的安装目录下，攻击者常将其[boot]字段的 shell=Explorer.exe 变为 shell=Explorer.exefile.exe。注意这里的 file.exe 就是木马服务端程序。

（3）利用注册表加载运行：注册表的很多位置都是木马藏身之所。

（4）在 Autoexec.bat 和 Config.sys 中启动：C 盘根目录下的这两个文件也可以启动木马。但这种方式一般都需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件，而且采用这种方式易被发现，所以这种方式并不多见。

（5）启动组：是木马隐藏的重要位置。

（6）制作好的带有木马启动命令的同名文件上传到服务端覆盖这些同名文件，达到启动木马的目的。

（7）修改文件关联：这种方法是木马常用的攻击手段。例如，正常情况下 TXT 文件的打开方式为 Notepad.EXE 文件，但一旦中了文件关联木马，则 txt 文件打开方式就被修改为用木马程序打开。不仅是 TXT 文件，其他诸如 HTM、EXE、ZIP.COM 等都是木马的目标。

（8）捆绑文件：这种方式的触发条件是首先要控制端和服务端已通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，然后上传到服务端覆盖源文件，这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马也会安装上去。

2. 木马的隐藏

（1）隐藏在任务栏。这是木马最基本的隐藏方式。

（2）隐藏在任务管理器。

（3）主机端口，大多数木马使用1024以上的端口进行通信，随着技术的发展，现在的木马都提供端口修改功能。

（4）隐藏通信。任何木马运行后都要和攻击者进行通信连接，可以通过即时连接，如攻击者通过客户端直接接入被植入木马的主机；或者通过间接通信，如木马把侵入主机的敏感信息送给攻击者。因此，要对客户端和服务端的通信进行隐藏。

（5）隐藏加载方式，木马通过对加载方式的隐藏，使得用户运行木马程序。随着网站技术的不断进步，木马的传播介质越来越多，几乎WWW的每一个新功能都可以被木马利用。

3．木马的特性

（1）木马包含在正常程序中，随着正常程序的运行而启动，具有隐蔽性。

（2）具有自动运行性。

（3）对系统具有极大危害性。

（4）具有自动恢复功能。很多木马程序可以进行多重备份，相互恢复。当删除其中某一个的时候，再运行其他程序的时候，木马就会出现。

4．木马的种类

根据木马的破坏功能不同，可以将木马分为以下几类，见表5-3。

表5-3　木马的种类

木马种类	描述
破坏型木马	其功能是破坏并且删除文件，可以自动删除用户电脑上的DLL、INI、EXE文件
密码发送型木马	有的用户喜欢把自己的各种密码以文件的形式存放在计算机中，还有的用户喜欢用Windows提供的密码记忆功能记忆密码，密码发送型木马可以找到这些文件，并把它们送到攻击者手中。也有些木马程序会长期潜伏，记录操作者的键盘操作，从中寻找有用的密码
远程访问型木马	可以实现远程控制，监视被控制主机的操作
键盘记录木马	这种木马能记录受控主机的键盘敲击并在LOG文件里查找密码
DoS攻击木马	被DoS攻击木马入侵的主机被攻击者控制成为“肉鸡”，向目标主机发动攻击。有一种类似于DoS的木马叫做邮件炸弹木马，一旦被感染，木马就会随机生成各种主题的信件，对特定的邮箱不停地发送邮件，直到对方瘫痪、不能接受邮件为止
代理木马	代理木马使得受感染主机变成了攻击者发动攻击的跳板。通过代理木马，攻击者可以在匿名的情况下使用Telnet、ICQ、IRC等程序，从而隐蔽自己的踪迹
程序杀手木马	这种木马的功能就是关闭对方主机上的防木马程序，保证其他木马能发挥更大作用
反弹端口型木马	一般的防火墙对于请求连入的链接会进行严格的过滤，而对请求连出的链接却疏于防范。反弹端口型木马就是针对这一性质开发的，其服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马服务端定时监测控制端的存在，发现控制端上线立即弹出端口主动连结控制端。为了隐蔽起见，控制端的被动端口一般开在80，即使用户使用扫描软件检查自己的端口，也不容易发现这种类型的木马

5.3.4 网络控件

对于恶意代码来说，互联网就是最为常见的进入口之一。现在的 Web 浏览器和其他的网络应用都依赖于能够提供大量复杂功能的可执行程序。这种插件程序可以很容易地保证系统处于最新状态并且能够支持很多新文件的类型。但是这些程序同样可以被某些人利用，使其很容易就将恶意代码发送到用户主机。因为互联网上连接着大量的主机，所以算得上是一个持续的威胁。作为用户，必须保证病毒扫描器和防御软件可以有效地保护系统不被恶意程序损坏。

5.4 常见的攻击类型

目前，比较流行和常见的攻击有后门攻击、暴力攻击、缓冲区溢出、拒绝服务攻击、中间人攻击、社会工程学和对敏感系统的非授权访问等。

5.4.1 后门攻击

后门是指对系统的一个特殊访问通道，后门攻击是指通过后门绕过软件的安全性控制从而获取程序或系统访问权的方法。后门通常是由程序的编写者留下的，目的在于更方便地完成软件的测试。这样就造成了某些安全隐患，一些道德败坏的程序编写者能够利用后门获取非授权的数据；另外，后门相当于访问控制的一个巨大漏洞，一旦被攻击者发现并利用就会造成巨大的损失。预防后门最好的方法就是通过加强控制和安全关联测试来检验后门是否存在，并在发现后门时及时采取措施。

5.4.2 暴力攻击

暴力攻击或称为穷举法，指通过尝试系统可能使用的所有字符组合来猜测系统口令。这种攻击方法不断地向访问控制发送可能的口令值，以寻找正确的口令获得系统的访问权。理论上利用这种方法可以破解任何一种密码，问题只在于如何缩短试误时间。因此有些人通过使用大型计算机增加效率，有些人通过字典来缩小密码组合的范围。这种方法的效率很低，当破译一个 10 位的密码时，由于密码包含数字，大小写字母，其可能的组合数以亿计，对于普通的处理器，可能会用掉几个月的时间。所以相对而言，攻击成本很高。

当然对付这种攻击的最好方法就是小心保管系统口令并在系统中设置允许输入口令次数的最大值，若超过这个数值，账号就会被自动锁定。同时要对登录行为进行日志记录，可以在日后用于调查。

5.4.3 缓冲区溢出

缓冲区溢出攻击是一种可预防的攻击，其攻击成功率一般取决于程序中存在的异常。总体来说，当存储的字符串长度超过目标缓冲区存储空间而覆盖在合法数据上时就会发生缓冲区溢出攻击。例如，将一个 20 字节的字符串复制到只有 10 字节的缓冲区。防止这种攻击最简单的方式就是在复制的时候检查数据的长度和缓冲区的长度，而这是每个编程者最容易忽略的。

目前有两种在地址空间中安排攻击代码的方法：植入法和利用已经存在的代码。

（1）植入法。攻击者向被攻击的程序输入一串字符串，程序会将这个字符串放到缓冲区，字符串内包含的可能是被攻击平台的指令序列，缓冲区可以设在任何地方：堆栈、堆或静态存储区。

一个成功的缓冲区溢出攻击可以导致程序的异常和崩溃。如果将 20 个字符复制到 10 个字符的缓冲区，多余的 10 字符就会放在缓冲区后面 10 字符的空间里造成内存的重写，而重写内存能够直接导致程序的崩溃。这种类型的攻击相当普遍，因为在系统中运行的大量程序都存在着这种脆弱性。攻击者通过扫描系统获得系统运行程序的信息，然后就可以利用程序已知的脆弱性进行攻击了（www.securityfocus.com 中有关于程序已知脆弱性的大量记录）。

（2）利用已经存在的代码。很多时候，攻击者需要的代码已经存在于被攻击的程序中，攻击者要做的就是传递一些参数，比如，攻击代码要求执行“exec (bin/sh)”，而在 libc 库中的代码执行“exec (arg)”，其中 arg 是指向字符串的指针参数，那么攻击者只要把传入的参数指针改向指向“/bin/sh”即可。

5.4.4 拒绝服务攻击

拒绝服务攻击就是用于摧毁系统的可用性，此类攻击往往导致系统过于繁忙以至于没有能力去响应合法的请求。拒绝服务攻击有很多种方式，一类是基于漏洞的攻击，发送少量数据导致目标资源被大幅占用，漏洞可能会是操作系统的漏洞，应用软件的漏洞，也有可能会是 IP 协议的漏洞；还有一类是面向网络资源的攻击，即通过控制大量傀儡主机对目标主机发送正常报文导致目标系统的资源耗尽。大部分的拒绝服务攻击就是向目标主机发送请求响应的网络数据包。当然无论出于什么形式，最终的目标都是拒绝访问。

目前拒绝服务攻击多为分布式拒绝服务攻击（DDos），其将多个计算机联合起来作为攻击平台，对一个或多个目标发动拒绝服务攻击，从而成倍的提高拒绝服务攻击的威力。例如，一名攻击者使用一个非授权账户将 DDos 主控程序安装在计算机上，同时将代理程序安装在互联网的其他计算机上，代理程序在某个时间段内受到指令发动进攻，最终破坏目标系统的可用性。

而与 DDos 配合使用最多的就是 SYN Flood 攻击，其利用 TCP 协议的安全缺陷，发送大量伪造的 TCP 连接请求，使被攻击方的资源耗尽。具体来说，SYN Flood 是通过三次握手实现的。

（1）攻击者想被攻击服务器发送一个含有 SYN 标志的报文，SYN 会指明客户端使用的端口以及 TCP 连接的初始序号，这是攻击者与被攻击者建立第一次的握手。

（2）被攻击服务器受到攻击者的 SYN 报文后，将返回一个 SYN-ACK 的报文，表示攻击者的请求被接受，同时 TCP 序号加 1，ACK 被确认，这是攻击者与被攻击者之间建立的第二次握手。

（3）服务器在发送应答报文后无法收到攻击者的 ACK 报文，一般情况下服务器会重试，这时候服务器会等待一段时间。作为一个攻击者，让服务器等待一段时间对服务器的运行没有太大的影响，而如果恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗资源。即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试，即使服务器的性能足够强大，也会随着 CPU 的效率不断降低导致无法处理其他客户的正常请求，这种情况下，服务器段就属于遭受了拒绝服务攻击。

5.4.5　中间人攻击

中间人攻击是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，然后把这台计算机模拟一台或两台原始计算机，使“中间人”（入侵者放置的计算机）能够与原始计算机建立活动连接，而两台原始计算机用户却意识不到“中间人”的存在，只以为是和彼此进行通信。“中间人”通过假冒身份，可以截获原始计算机的通信消息，进而进行一系列的攻击。

例如，有 3 台终端同时连接到同一个工作组交换机中。此时如果主机甲需要访问主机乙（第一次访问时只知道对方的 IP 地址而不知道 MAC 地址），就需要先发送一个 ARP 请求。向各台主机询问，IP 地址为多少的主机其 MAC 地址为多少，并会附上主机甲的 MAC 地址。ARP 请求会以广播的形式在局域网中传播。正常情况下，除了乙以外的不相关的主机都会丢弃这个数据包。而只有主机乙接收到这个请求后，才会进行响应。主机乙首先会在自己的 ARP 缓存中创建主机甲 IP 地址与 MAC 地址的相关记录（如果已经存在这个 IP 地址，则会进行更新），并向主机甲发送 ARP 响应。此时的 ARP 响应是一个单播数据包，即直接发送给主机甲，而不是以广播的形式发送。以上是正常的 ARP 处理流程。但是在这个过程中，如果终端设备丙在收到主机甲发送的 ARP 请求之后，没有抛弃这个数据包，而是发送了伪造的 ARP 响应（将自己的 MAC 地址替代主机乙的 MAC 地址），同时阻扰主机乙的正常通信，那么就可以发起中间人攻击。甲在接收到主机丙的 ARP 响应之后，将不能够拥有主机乙的正确 MAC 地址与 IP 地址。对于主机甲来说，它就会错误的认为主机丙就是其要发送数据的对象。从而将数据直接发送给主机丙。此时对于主机甲和主机乙之间的任何通信，就会被发送到主机丙上。然后主机丙在获取相关的内容之后，可能进行流量的重定向。在这个过程中，主机丙就被称为中间人。这个过程就被称为中间人攻击。

5.4.6　社会工程学

社会工程学是一种利用被攻击者心理弱点、本能反应、好奇心、信任、贪婪等心理

而设置陷阱，以交谈、欺骗、假冒等方式，从合法用户中套取用户系统秘密的一种攻击方法。一个攻击者通常会利用各种手段欺骗用户泄露系统口令或说服用户在其主机上安装木马。由于动作的执行人的确是系统授权用户，因此这种类型的攻击很难被监测到。对付这种类型的攻击最有效的方法就是加强安全意识教育。要让用户记住任何情况下都不能向其他人泄露自己的口令，任何想要进入系统的用户都应该被及时报告给上级。通过这些简单的规则可以有效地降低社会工程学的攻击。

5.4.7　对敏感系统的非授权访问

大部分攻击的目标都是访问系统的敏感信息。一种情况是攻击者获取具有经济价值的信息，例如关于某个投资项目竞标的信息；另一种情况是攻击者只想修改信息，例如在某次考试中成绩不理想的同学，就会想办法进入成绩数据库，将自己的成绩信息进行修改。

无论是处于哪种目的，对敏感信息的非授权访问都会对系统造成严重的损害。

5.5　无线网络安全

5.5.1　无线网络基础

无线网络技术诞生于 1970 年，40 年来，随着通信技术的不断发展，无线网络技术也作为提升最快的通信技术之一进入大众的视野。无线通信技术可以在区域内实现移动通信，为了满足这种通信的需求，无线网络的基础设施、通信技术都有了很大发展。

目前，无线局域网采用的传输媒体主要有两种，即红外线和无线电波。按照不同的调制方式，采用无线电波作为传输媒体的无线局域网又可分为扩频方式与窄带调制方式。

5.5.2　无线网络协议标准

无线网络协议标准主要为 802.11 系列协，是由 IEEE 制定的，目前居于主导地位的无线局域网标准，其包括 IEEE802.11b、IEEE802.11a、IEEE802.11g、IEEE802.11n，图 5-3 给出了每一个标准的相关参数。

5.5.3　无线网络安全

如今，无线网络技术已经广泛应用到多个领域，然而，无线网络的安全性也是最令人担忧的，经常成为入侵者的攻击目标。WEP（Wired Equivalent Privacy）和 WPA（ Wi-Fi Protected Access）是无线网络安全中最重要的两个安全加密模式。

无线技术与标准	802.11	802.11a	802.11b	802.11g	802.11n
推出时间	1997 年	1999 年	1999 年	2002 年	2006 年
工作频段	2.4GHz	5GHz	2.4GHz	2.4GHz	2.4GHz 和 5 GHz
最高传输速率	2Mbps	54Mbps	11Mbps	54Mbps	108Mbps 以上
实际传输速率	低于 2Mbps	31Mbps	6Mbps	20Mbps	大于 30Mbps
传输距离	100M	80M	100M	150M 以上	100M 以上
主要业务	数据	数据、图像、语音	数据、图像	数据、图像、语音	数据、语音、高清图像
成本	高	低	低	低	低

图 5-3　802.11 系列协议的实际参数

1. WEP

WLAN（无线网络）的一个目标就是提供与有线网络等同的安全性，为了达到这个目标，无线网络标准的设计者们提出了多种安全机制来提供数据的保密性服务，身份认证服务和访问控制服务。对于 IEEE802.11 标准来讲，加密与验证都是建立在 WEP 算法上面的。

WEP 算法通过一个长度为 40 位的密钥来提供身份认证与加密。在 WEP 安全机制中，同一无线网络的所有用户和接入访问点（AP）使用相同的密钥来加密和解密，网络中的每个用户和 AP 都存放着一份密钥。802.11 标准没有定义一种密钥管理协议，所以 WEP 密钥必须通过手工进行管理。WEP 算法是一种由明文与其等长的伪随机密钥序列按位进行模二相加来获取密文的算法。WEP 机制采用了 40 位或 104 位的加密密钥，与 24 位的初始化向量 IV 连接，产生 64 位或 128 位密钥种子，然后送入一个伪随机产生器 PRNG，用生成的伪随机序列对传输的明文数据进行加密。该系统同时还采用 CRC-32 作为完整性校验的校验值。

图 5-4 给出了无限网络采用 CRC-32 完成完整性校验的具体过程。

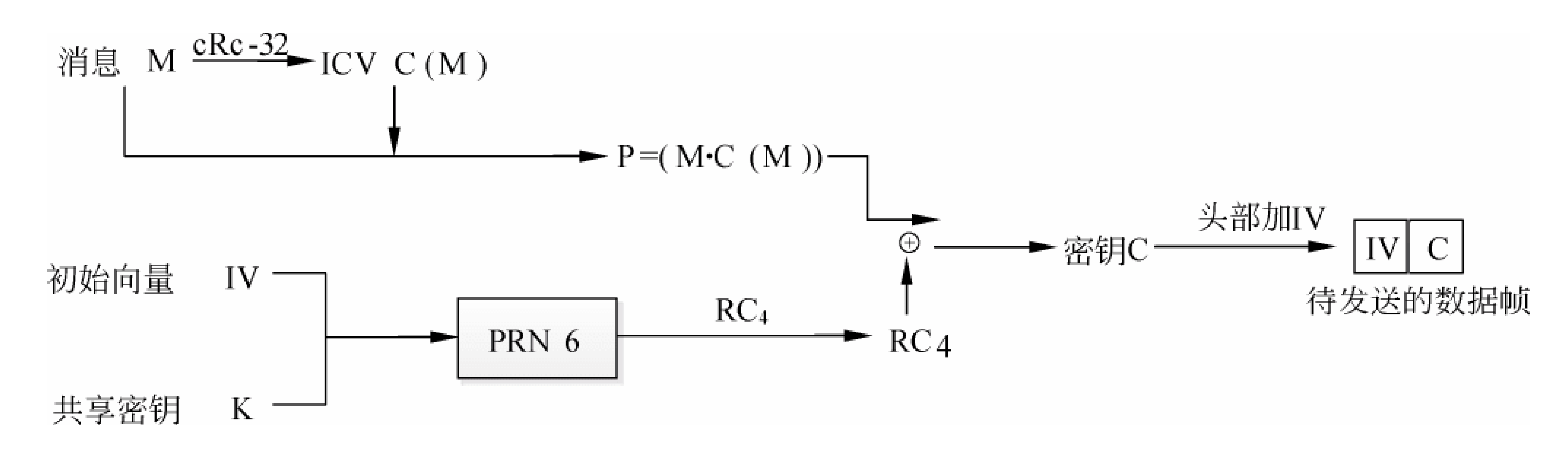


图 5-4　无线网络的完整性校验

（1）校验和计算：根据待发送消息 M 的二进制码流通过 CRC-32 计算出完整性检验值 ICV C(M)，然后把 C(M)附在原始明文 M 的尾部，组成完整的明文 P=<M，C(M)>。

（2）密钥流生成：选择一个 24 位的初始向量 IV，由 IV 和 40 位的共享密钥 K 组成

64 位的密钥流种子，将 64 位的种子输入伪随机序列产生器 PRNG，经过 RC4 算法生成密钥序列或称为密钥流，它是初始化向量 IV 和密钥 K 的函数，表示为 RC4(IV，K)。

（3）数据加密：将明文 P=<M，C(M)>和密钥流 RC4(IV，K)相异或得到密文 C，其数据表达式为：C=P ⊕ RC4(IV，K)，其中 P=<M，C(M)>。

（4）数据传输：在密文 C 的头部附上 IV，得到待发送的数据帧，然后通过无线方式将其发送到接收端。

数据解密链路层数据的解密过程是加密过程的逆过程。在接收端，密钥流 RC4(IV，K)将被重新生成，与密文 C 相异或便可得到明文 P"。接收方把解密后的明文 P"分解成消息 M"和校验值 C(M)"，并由 M"计算出校验和 C(M")，比较 C(M")和收到的校验和 C"是否一致，如果一致，则接受此数据帧；否则，将其丢弃。

2. WPA

WPA 是一种保护无线网络（Wi-Fi）安全的系统，它是在研究者在前一代的系统 WEP 中找到的几个严重的弱点的基础上而产生的，它有 WPA 和 WPA2 两个标准。

WPA 的数据是以一把 128 位元的钥匙和一个 48 位元的初向量(IV)的 RC4 流密码来加密。针对 WEP 的缺点，WPA 做的主要改进就是在使用中可以动态改变钥匙的“临时钥匙完整性协定”（Temporal Key Integrity Protocol，TKIP），加上更长的初向量，这可以击败许多针对 WEP 的攻击，如知名的金钥撷取攻击。

除了加密和认证外，WPA 对于所载数据的完整性也提供了巨大的改进。WEP 所使用的 CRC（循环冗余校验）先天存在不安全性缺点，在不知道 WEP 钥匙的情况下，要篡改所载数据和对应的 CRC 是完全可能的，而 WPA 使用了称为“Michael”的更安全的讯息认证码（在 WPA 中叫做讯息完整性查核，MIC）。此外，WPA 使用的 MIC 包含了帧计数器，以避免 WEP 的另一个弱点——回放攻击的利用。

WPA 的增大钥匙和初向量、减少和钥匙相关的封包个数、再加上安全信息验证系统使得侵入无线局域网路的难度大大增加。Michael 算法是 WPA 设计者在大多数旧的网卡也能使用的条件下找到的最强的算法，但是它可能会受到伪造封包攻击。为了降低伪造封包攻击的风险，WPA 网络每当侦测到一个企图的攻击行为时就会关闭 30 秒钟。

5.5.4 无线局域网存在的安全问题

无线网络有其固有的不安全性，总体看来，WLAN 面临的安全问题主要有以下几个方面。

1. 身份标识

身份标识是安全机制中一个很重要的部分。WLAN 的协议栈中包含着一个介质访问控制协议层，WLAN 标准通过比较试图连接到路由器的设备的 MAC 地址和路由器所保存设备的 MAC 地址来判断是否允许进入网络。当然这种方法不是绝对安全的，例如入侵者可以通过克隆 MAC 地址来试图连接网络。

另外 WLAN 也使用服务集标识（SSID）来标识自己的无线路由设备，设置了 SSID

的路由设备必须由设置了相应的SSID的用户才可以进入网络。简单地说，一个SSID就是一个无线局域网的名称，只有相同SSID值的电脑才能互相通信。值得注意的是，每一个厂商的无线设备都有一个默认的SSID，攻击者可以利用这些SSID来渗透无线局域网。

2．缺乏访问控制机制

无线局域网标准本身不包括任何访问控制机制，为了修补这一安全漏洞，大部分无线设备都使用基于MAC地址的访问控制列表（ACL），列表将每一个允许通过的MAC地址列举在其目录下，如果MAC地址不在ACL中，那么该客户端就会被拒绝访问该网络。但攻击者可以通过更改本身的MAC地址进入网络。攻击者首先监听一个有效的MAC地址的通信或者通过无线嗅探软件捕获网络中正在使用的MAC地址列表，然后将自己的MAC地址进行伪装，这样就可以以合法的身份进入无线网络中。

3．802.11标准中缺乏认证机制

802.11标准支持两种认证服务：开放型系统与共享密钥。认证类型由认证类型控制参数控制。开放型系统是一个默认的认证算法，包含两个步骤：第一步是在访问控制接入点向客户端索取身份标识；第二步是通过认证服务器认证客户端的请求。在这种认证方式中，无线接入点只起到了传递的功能，所有的认证工作在申请及认证服务器上完成。

在共享密钥认证模式下，客户端通过挑战应答的方式通过认证。802.11要求客户端使用秘密信道进行认证，首先客户端会发送一个“认证请求管理数据包”，说明想要使用共享密钥，接入点收到该请求后，会发送一个“认证管理数据包”作为对客户端的响应，该数据包包含128个字符，伪随机数字生成器和一个随机的初始向量。伪随机数字生成器作用是生成带有共享密钥的质询文本，随后，该客户收到认证管理数据包将质询文本复制到一个新的数据包中，并选择一个新的初始变量将其放在含有质询文本的数据包中进行WEP加密并传输给接入点。接入点收到给数据包后，通过共享密钥对其进行解密，并查看32位的CRC完整性校验值以验证数据包的完整性。验证成功后，为达到相互鉴别的目的，客户与接入点互换角色重复以上过程。

4．WEP密钥的管理问题

802.11无线局域网本身不支持加密与认证服务，这些服务机制都是通过WEP来提供，因此对无线局域网来说，WEP密钥管理的缺失是另一个较为重要的安全漏洞。另外由于大型网络架构包含众多漫游基站与客户端，而相互之间缺乏内部访问协议，使得IEEE802.11已经不能满足一些大型网络的安全需求了。

5.6 传感网络

无线技术在近些年的发展，推动了低功耗多功能传感器的快速发展。无线传感网络或者说传感网络是指相互合作的多个独立设备以自组织的形式构成网络，并通过多跳中继方式将监控数据传到汇聚节点。这些相互合作的独立设备在传感网络中称为传感器，

用于侦查、监督、追踪周边环境变量，如不同地点的温度、声音、振动和压力。

随着技术的发展，传感网络中的节点已经能够装载一些小程序在将收集到的数据传送给汇聚节点之前对其进行简单的处理；传感节点之间也出现了一些复杂的协议，可以有效地降低节点之间通信的无谓损耗；数据收集的准确度也得到了大幅度的提升。这些技术的使用节约了汇聚节点的操作使其有更多空间处理传入的数据。

5.6.1 传感网络的基本元素

作为一种新型网络，传感网络的基本要素有以下这些内容。

- **路由** 无线传感网络的通信与传统网络通信相似，同样是基于多层次的协议栈的通信。目前广泛使用的路由协议包括：以数据为中心的路由协议，分层次的路由协议和基于地点的路由协议。
- **功耗** 由于大部分的传感节点都处在不可达环境中，所以对其进行能量补充就很困难。当一个传感节点的能量用光时，工作就会失效。因此，对于一个网络来说，其性能高低和传感节点计算效率关系极大。
- **容错性** 任何传感网络的可靠性必须强，能够不受单个节点错误的影响。
- **可扩展性** 当有新的节点加入时，传感网络应该不受影响。
- **生产成本** 无线传感网络通常使用大量的传感节点，每个独立的传感节点都关系着整个传感网络的成本。
- **传感网络的拓扑结构** 任何一个普通传感网络都会包含着数千个传感节点，这数千个传感节点会随机分布在网络的各个地点，节点部署方式不同也会导致区域内节点的密度不同进而影响网络的性能，因此无线传感网络的拓扑结构也极其重要；传输介质：在无线传感网络中，节点之间通过无线网络进行连接，这个无线介质可能是红外、蓝牙、无线射频或光波，它们的传播效率决定着传感网络的性能。

5.6.2 无线传感网络安全

1. 无线传感网络的安全需求

无线传感网络由于具有分布在各处的节点，所以其安全需求也于传统的系统安全有些不同，具体如下。

- **节点的物理安全性** 虽然无法保证节点物理上的绝对不可破坏，但可以采取一定的措施增加节点被破坏的难度，并加强对节点数据的保护。
- **真实性、完整性、可用性** 需要保证通信双方的真实性以防止恶意节点冒充合法节点达到攻击目的，同时要保证各种网络服务的可用性。另外还要保证数据的完整性和时效性，对于一些特定的应用还要保证数据的保密性。
- **安全功能的低能耗性** 由于常用的加解密和认证算法往往需要较大的计算量，在应用到无线传感网络中时需要仔细衡量资源消耗和达到的安全强度，选择合适的算法以尽量小的资源消耗得到较好的安全效果。

- **节点之间的合作性** 无线传感网络中的许多应用都需要节点间保持一定的合作，但节点趋向于尽量降低资源消耗的特点与其合作性有一定的矛盾。
- **攻击容忍性** 单点失败或恶意节点的不合作行为，使得拓扑发生变化从而导致路由错误，需要无线传感网络具有自我组织性以避免此种情况。另外，网络也需要能容忍伪造、篡改、丢弃包等恶意行为。
- **攻击发现和排除** 无线传感网络应能及时发现潜在的攻击行为，并尽快消除恶意行为给网络带来的影响，比如隔离恶意节点将攻击流量拦截在网络之外，以收回被攻击者占据的网络资源。

2. 无线传感网络的安全机制

- **抗干扰** 攻击者可以通过干扰等手段对网络中的传感节点进行拒绝服务攻击，所以必须引入抗干扰的协议与服务来制止这种攻击的发生。
- **访问控制** 对用户授予合适的权限来访问传感网络的资源，对一个传感网络来说，访问控制机制是相当重要的。
- **密钥管理** 密钥管理是无线传感网络中的认证与加密服务的核心，随着传感网络应用的增加，一个有效的密钥管理方案是必须的。
- **数据备份** 能够在攻击发生情况下保证数据的完整性和可用性。
- **抗节点劫持** 传感网络面临的一个重要安全问题就是节点劫持，与传统网络物理安全可以得到很好的满足的特性不同，传感网络节点部署环境一般很难保证其物理安全。因此一般采用节点冗余或路由冗余的方案避免节点劫持。

习　　题

一、选择题

1. 以下哪一项不属于恶意代码？（　　）
   A. 病毒
   B. 特洛伊木马
   C. 系统漏洞
   D. 蠕虫

2. 使授权用户泄露安全数据或允许非授权访问的攻击方式称做（　　）。
   A. 拒绝服务攻击
   B. 中间人攻击
   C. 社会工程学
   D. 后门攻击

二、简答题

1. 病毒与蠕虫有何区别？试举例常见的病毒和蠕虫。
2. 简述 WEP 算法原理。
3. 常见的攻击类型有哪些？该如何防范这些攻击？

课后实践与思考

网站常见攻击实例

一、X-scan 扫描工具的使用

实验内容：

1. 使用 X-scan3.3 检测系统漏洞

2. 使用 X-scan3.3 扫描系统端口
3. 使用 X-scan3.3 检测系统用户以及共享信息

实验步骤：

1. 使用 X-scan3.3 检测系统漏洞

（1）设置要扫描的主机 IP 地址，如图 5-5 所示。



图 5-5　设置要扫描的主机 IP

（2）设置中选择扫描模块，如图 5-6 所示。



图 5-6　选择扫描模块

（3）全局设置中的其他选项可以按照默认，然后展开“插件设置”，选择“漏洞检测脚本设置”项，这里默认选择的是全部的脚本列表，如图 5-7 所示。

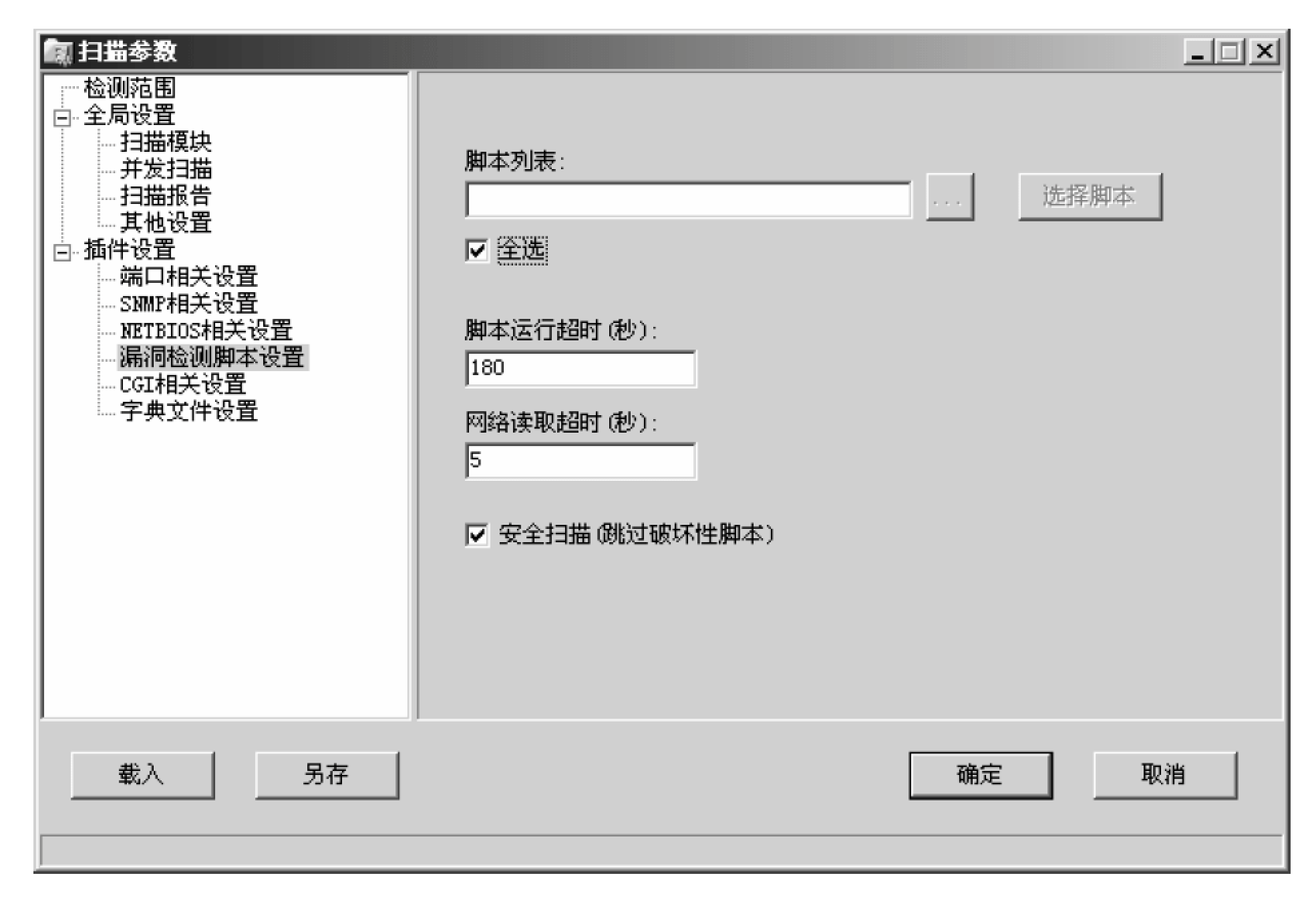


图 5-7　漏洞检测脚本设置

（4）脚本选择框中选择需要检测的脚本，如图 5-8 所示。



图 5-8　选择需要检测的脚本

（5）选择好后单击两次“确定”按钮退出扫描设置，然后单击“开始扫描”按钮，

如图 5-9 所示。

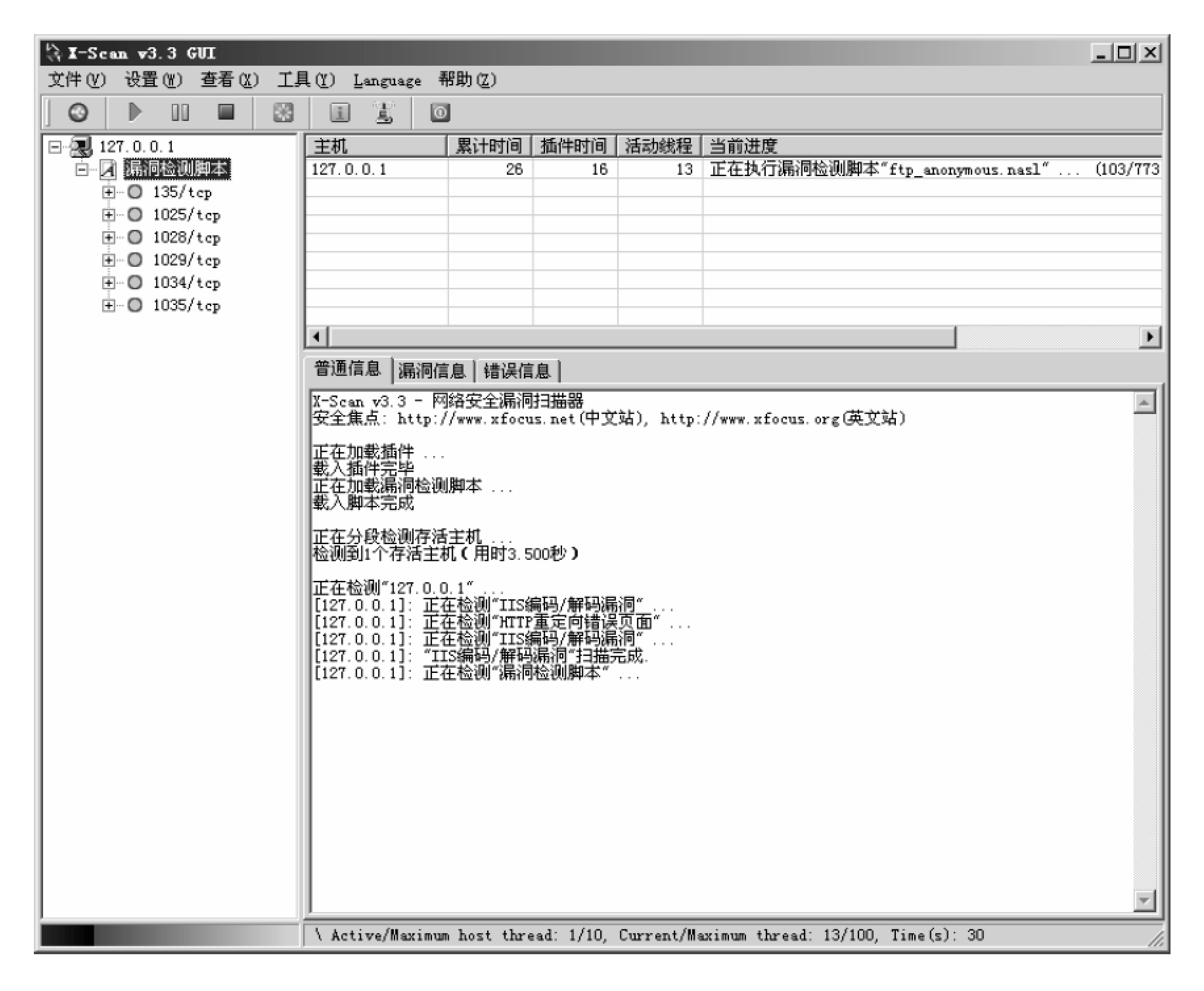


图 5-9　开始扫描

（6）扫描完成后会生成一个报告并以网页形式显示在 IE 浏览器中，如图 5-10 所示。



图 5-10　扫描报告

2. 使用 X-scan3.3 扫描开放的端口

（1）选择扫描模块，如图 5-11 所示。



图 5-11　选择扫描模块

（2）在端口设置中输入需要检测的端口，如图 5-12 所示。

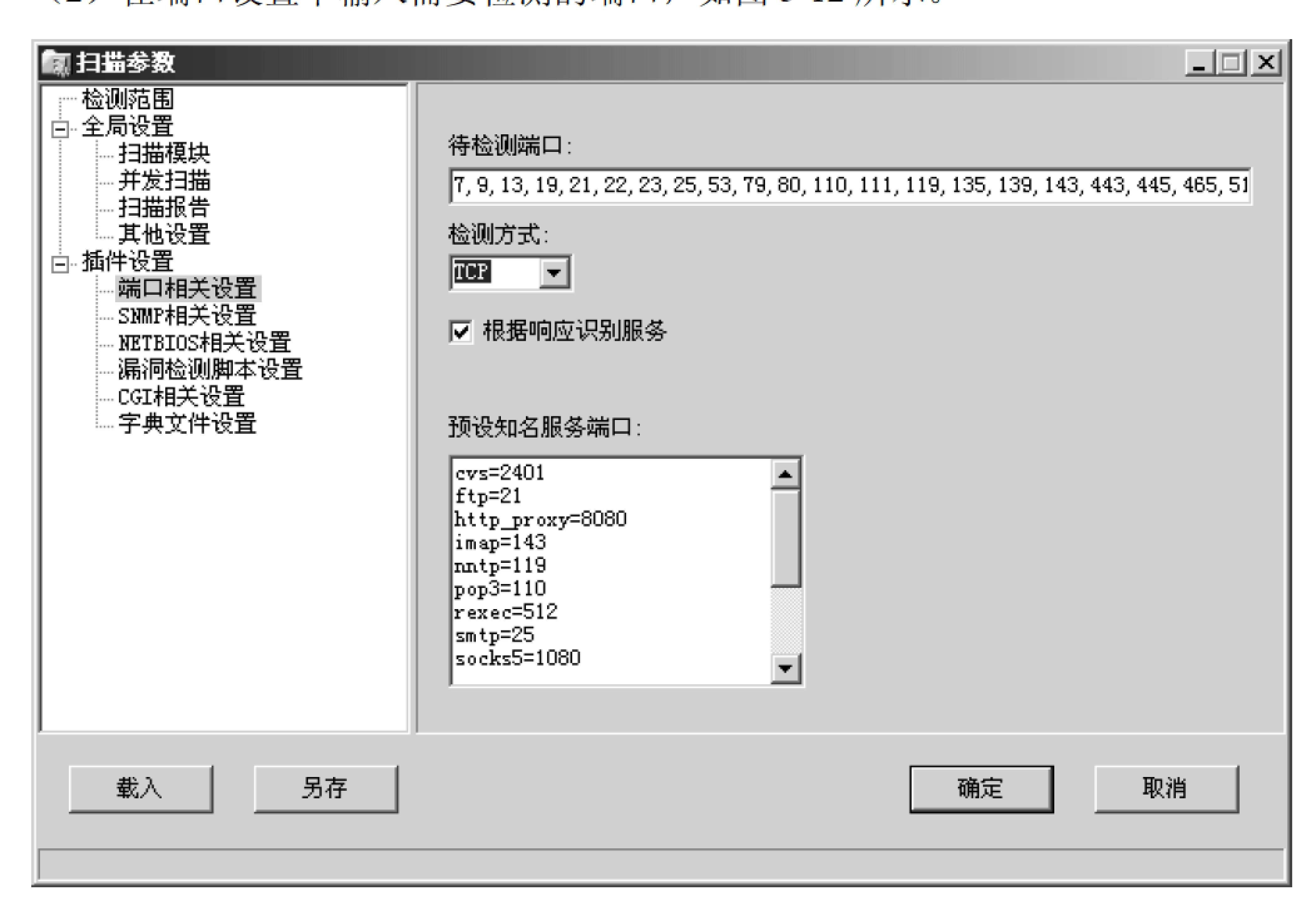


图 5-12　设置检测端口

（3）扫描过程如图 5-13 所示。

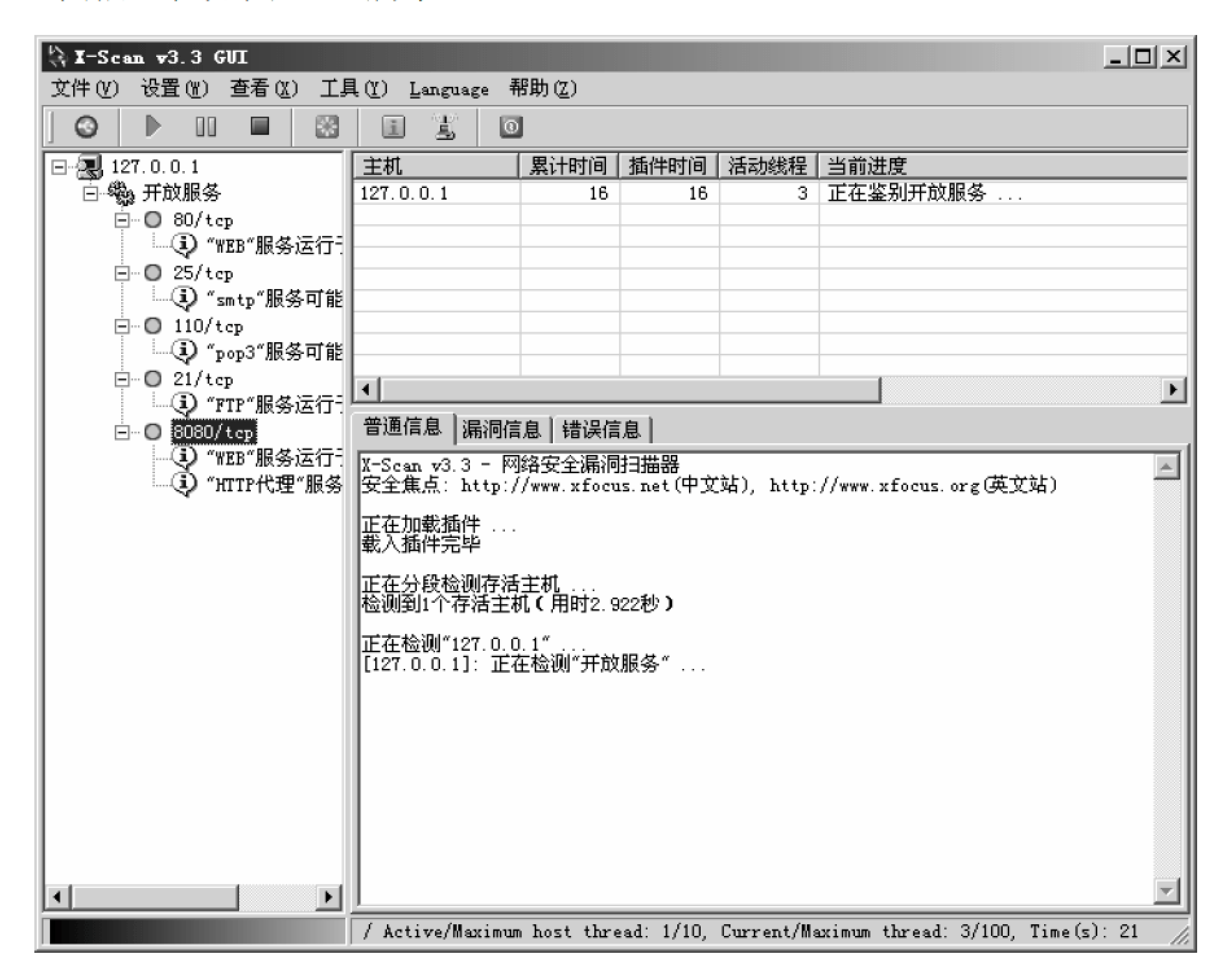


图 5-13 扫描过程

（4）扫描完成后查看生成的报告，如图 5-14 所示。



图 5-14 扫描报告

3. 使用 X-scan3.3 检测系统用户以及共享信息

（1）选择扫描模块，如图 5-15 所示。



图 5-15　选择扫描模块

（2）设置 NETBIOS 信息，如图 5-16 所示。



图 5-16　设置 NETBIOS 信息

（3）扫描过程如图 5-17 所示。

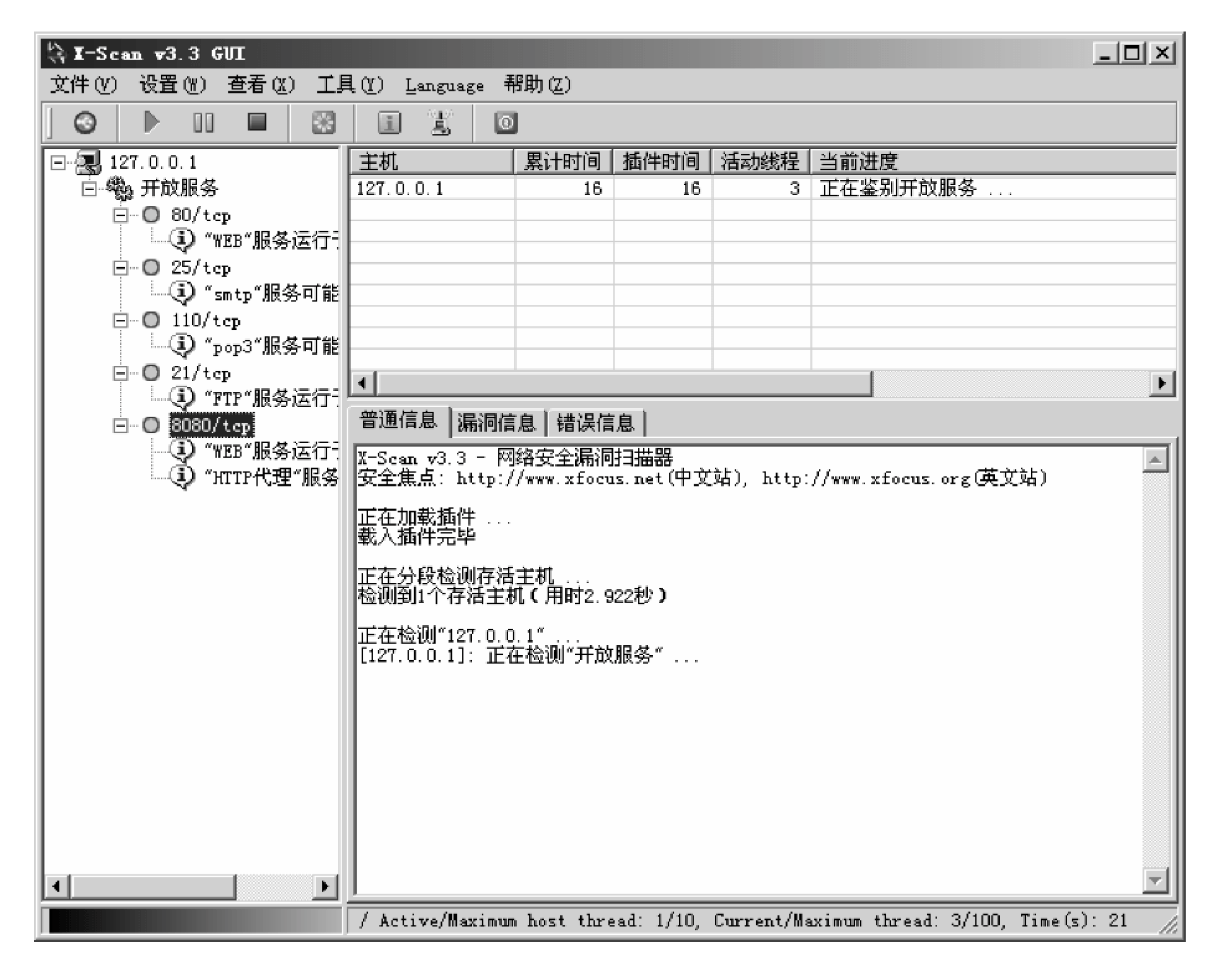


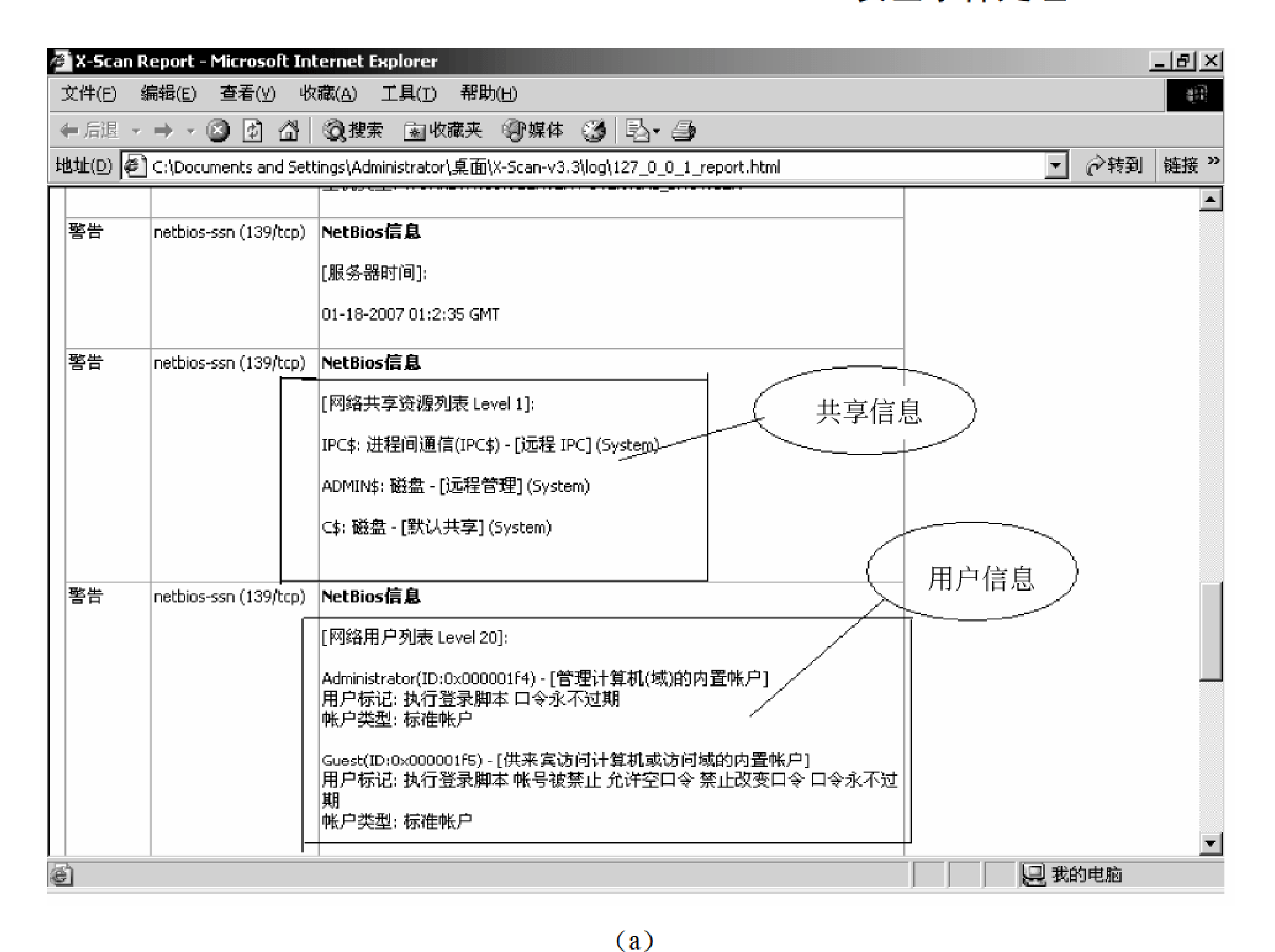
图 5-17　扫描过程

（4）扫描完成后查看生成的报告，如图 5-18 所示。

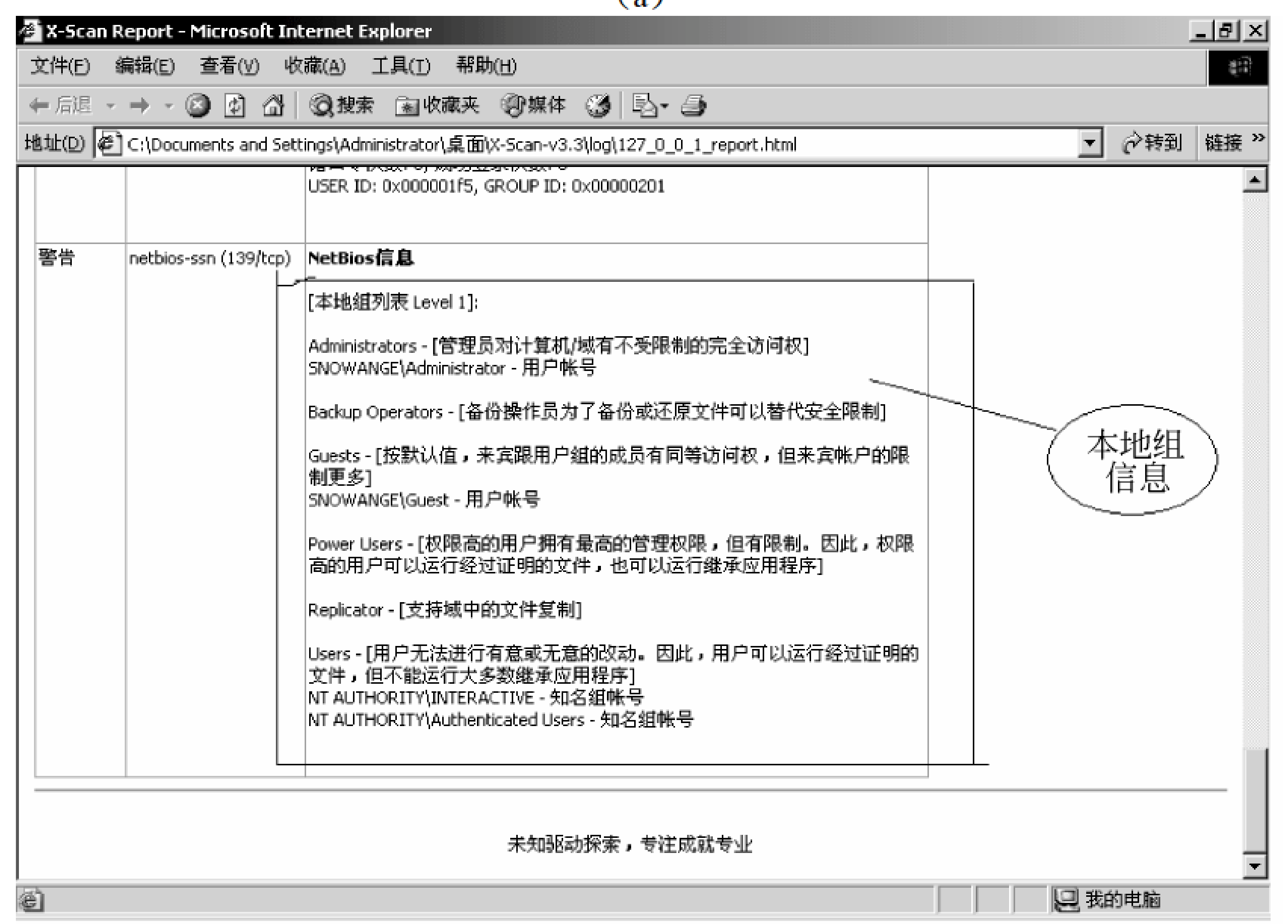


图 5-18　扫描报告

（5）扫描结果如图 5-19 所示。



(a)



(b)

图 5-19 扫描结果

二、DDos 对电子商务网站的攻击

实验内容:

模拟使用 DDos 对电子商务网站的攻击

实验步骤：

（1）打开资源管理器查看资源占用情况，如图 5-20 所示。

（2）攻击前，访问目标网站查看是否能很快登录。

（3）设置攻击目标，如图 5-21 所示。



图 5-20　资源管理器



图 5-21　设置攻击目标

（4）测试攻击效果，如图 5-22 所示。

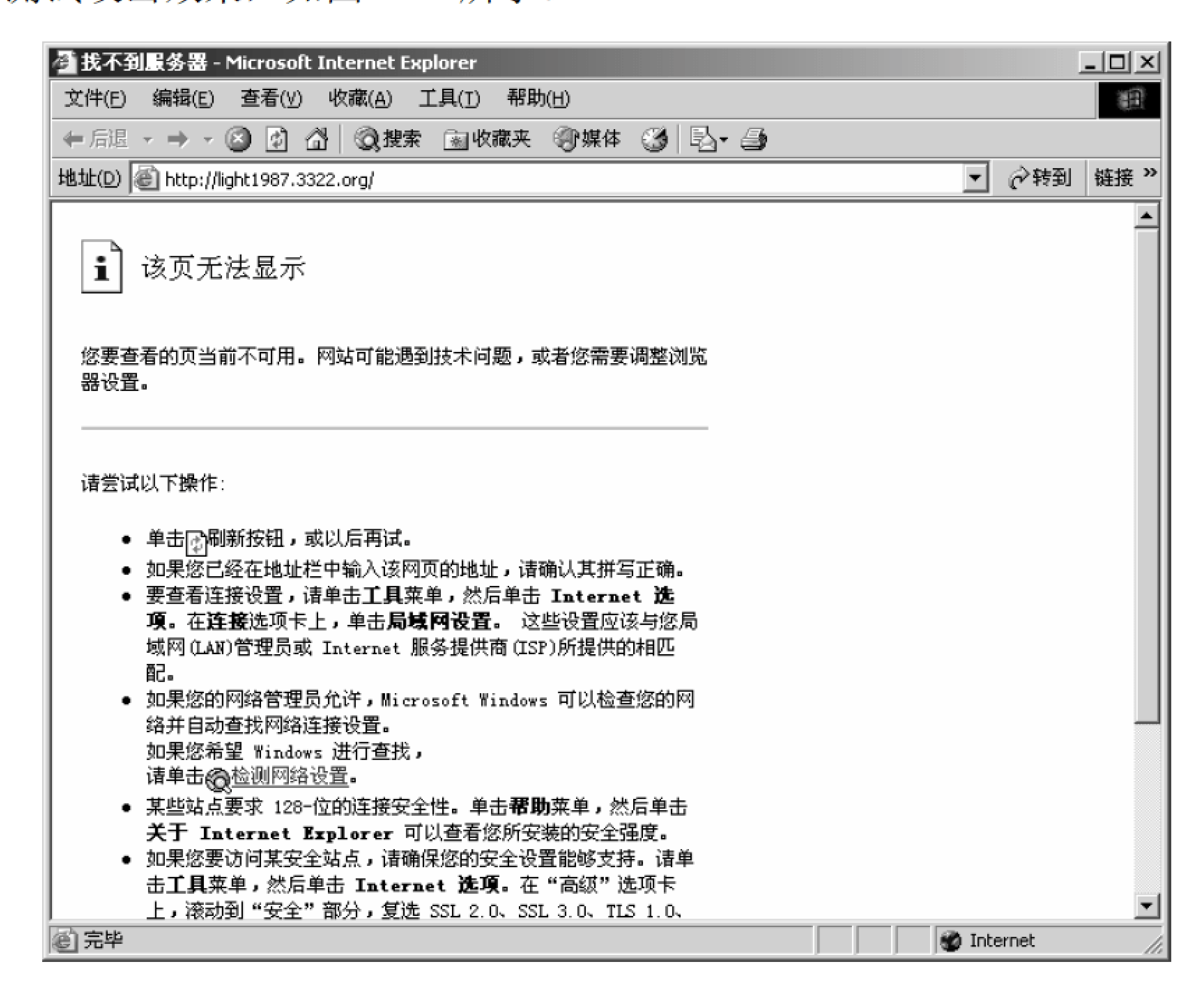


图 5-22　测试攻击效果

（5）查看资源占用，如图 5-23 所示。

（6）停止攻击，如图 5-24 所示。



图 5-23　查看资源利用

图 5-24　停止攻击

（7）停止攻击后，可成功访问网站，如图 5-25 所示。

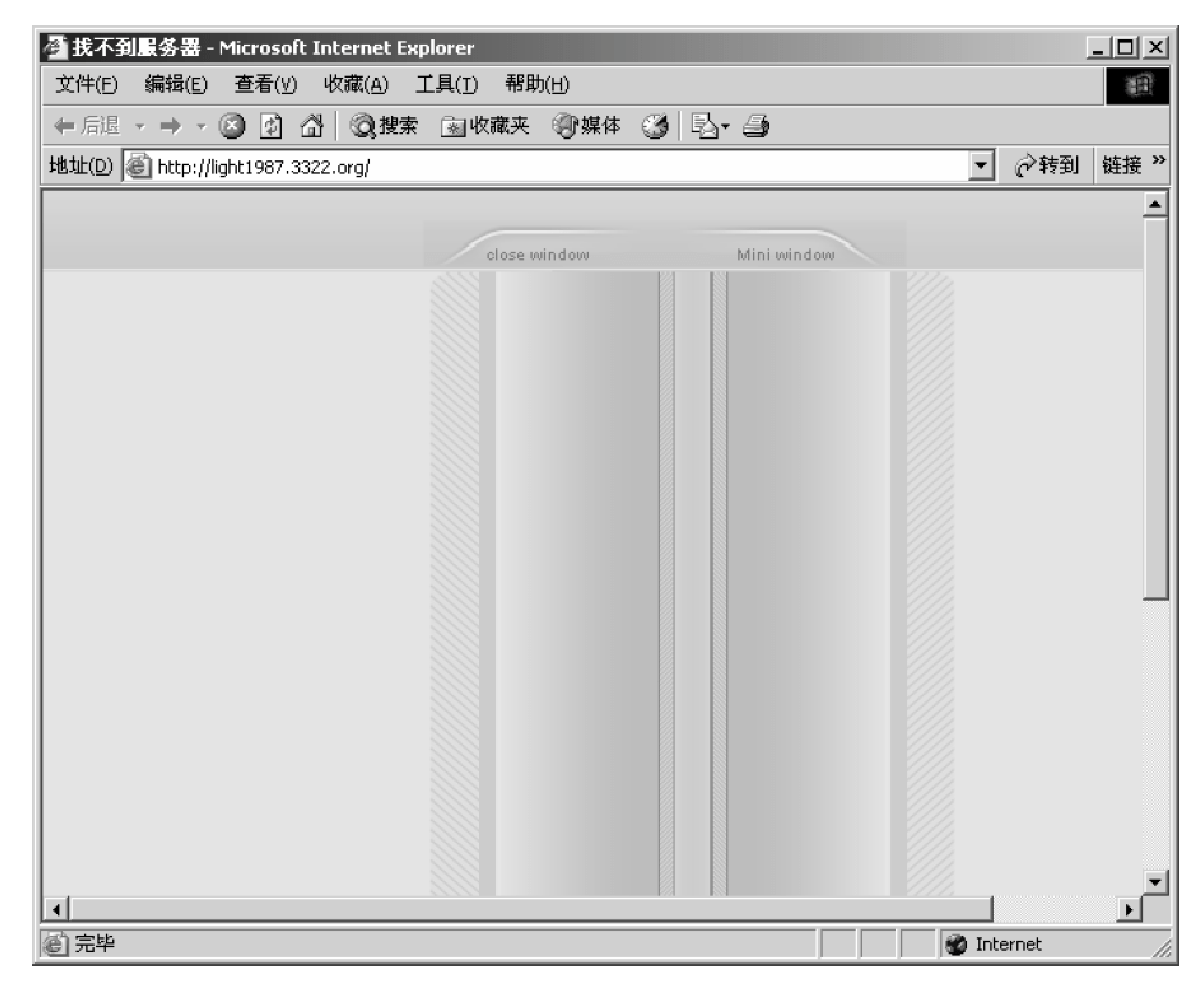


图 5-25　成功访问网站

第 6 章　访问控制与权限设置

本章学习重点：

- 理解访问控制的基本概念
- 掌握常见的访问控制技术
- 识别与比较访问控制模型
- 识别常见攻击类型，并熟悉相应解决办法

6.1 访问控制基本概念

访问控制是一系列用于保护系统资源的方法和组件，依据一定的规则来决定不同用户对不同资源的操作权限，可以限制对关键资源的访问，避免非法用户的入侵及合法用户误操作对系统资源的破坏。访问控制提供了系统的完整性和保密性。

访问控制由 4 部分组成：主体、客体、访问操作和访问监视器。主体指想要访问系统资源的用户或进程，由它发起访问请求。客体指主体试图访问的资源，客体可以是文件或内存、打印机、扫描仪这样的资源。访问操作有很多种的形式，包括网络访问、服务器访问、内存访问以及方法调用。合理的访问控制策略目标是只允许授权主体访问被允许访问的客体。

图 6-1 表示一个访问控制的一般过程。主体创建一个访问系统资源的访问请求，然后将这个请求提交给访问监视器。访问监视器通过检查一定的访问策略，决定是否允许这个访问请求。如果主体的访问请求符合访问策略，主体就被授权按照一定的规则访问客体。

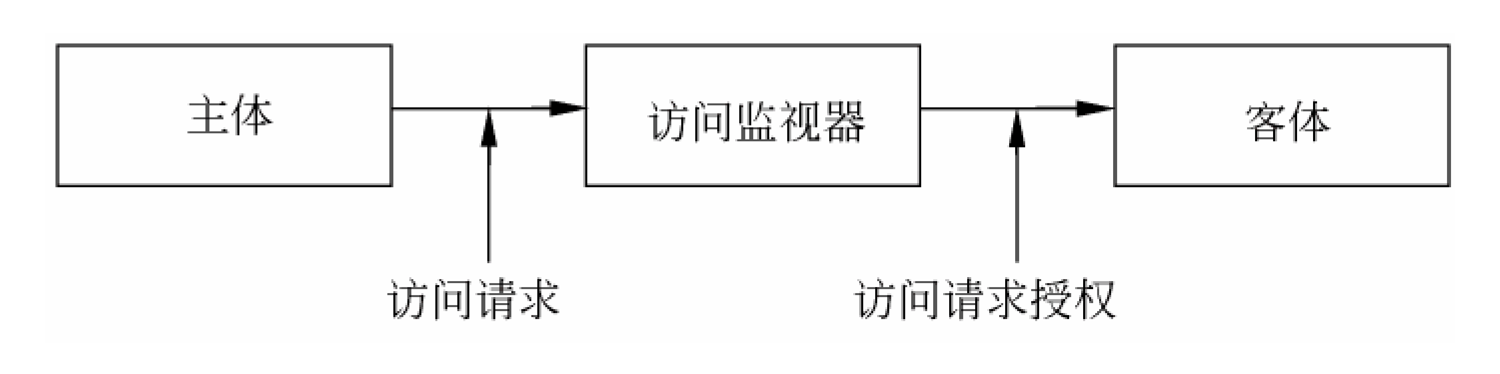


图 6-1　访问控制的一般过程

6.2 访问控制规则的制定原则

制定合理的访问控制规则是访问控制有效实施的基础，对保护系统安全起着重大作用。在制定访问控制规则时一般要遵守 3 条原则。

1. 最小特权原则

最小特权原则是指主体仅只被允许对完成任务所必需的那些客体资源进行必要的操

作，此外不能对这些资源进行任何其他的操作，同时也不能访问其他更多的资源。例如学校期末考试成绩数据库对于不同的访问者设置了不同的访问权限。一个学生访问数据库的时候就只有查询成绩的权限。而作为老师，除了拥有查询的权利外，还拥有成绩上传的权利。这个例子就很好地说明了最小特权原则。最小特权原则能够防止主体超出访问权限的越权行为，同时也避免了误操作对客体的威胁。

2．职责分离原则

在访问控制系统中，不能让一个管理员拥有对所有主客体的管理权限。要把整个系统分为几个不同的部分，把每个部分的管理权限交予不同的人员。这样可以避免一个人由于权利过大，滥用职权，进而对系统造成威胁。可以设置系统管理员，系统安全员和安全审计员，使其相互监督、相互制约。

3．多级安全原则

系统应该对访问主体及客体资源进行分级分类管理，以此保证系统的安全性。在实施访问控制的时候，只有主体的安全等级比客体的安全等级更高的时候，才有权对客体资源进行访问。

6.3 访问控制分类

不同的访问控制策略提供不同的安全水平，安全管理员应根据组织的实际情况选择最适合的访问控制来提供适合的安全级别。除了技术的因素，在实施访问控制的时候，还要相应提高组织成员的安全意识，使其自觉接受并遵守访问控制规则。不管访问控制规则是多么严密，如果得不到有效执行，其安全价值还是会大打折扣。同时在实施访问控制时，还要考虑到用户实际操作的便捷性，要在安全性和便捷性之见达到平衡。

6.3.1 自主访问控制

自主访问控制是指由客体资源的所有者自主决定哪些主体对自己所拥有的客体具有访问权限，以及具有何种访问权限。自主访问控制是基于用户身份进行的。当某个主体请求访问客体资源时，需要对主体的身份进行认证，然后根据相应的访问控制规则赋予主体访问权限。自主访问控制是目前计算机系统实现最多的访问控制机制，比较流行的UNIX系统就是利用自主访问控制机制实现对系统资源的管理。

由于这种机制允许由资源的所有者自主对所拥有的资源进行管理，因此更加灵活，实施更加方便，适合于对安全性不高的环境。然而，这种方法更容易造成信息的泄露，并且存在着用户管理困难，资源管理分散的缺点。

6.3.2 强制访问控制

在强制访问控制中，每一个主体和客体都有自己的安全标记，基于主客体的安全标记实施相应的访问控制。安全标记通常有4个不同的等级，分别是公开、敏感、秘密和

机密。在这种方法中，主客体安全等级的赋予、修改以及访问控制规则都是由系统强制控制的，因此，安全性更高。但正是由于同样的原因，这种方法的灵活性较差。

强制访问控制是基于规则进行的。依据主体和客体的安全级别来制定访问控制规则，决定一个访问请求是被接受还是被拒绝。组织的实际情况不同，因此设置的访问控制规则也不相同，例如在有些组织的访问控制规则中，标记为“秘密”等级的主体只能访问同样标记为“秘密”的客体。而另一种情况可能是，标记为“秘密”等级的主体除了可以访问标记为“秘密”的客体之外，还可以访问安全等级更低的客体。

除了主体的安全级别需要与客体的安全级别匹配以外，很多系统还要求主体拥有对客体的访问需求。这个访问需求说明主体拥有访问特定客体来完成任务的权限。因此，访问是基于安全级别和特定的任务需求而被授予的。

6.3.3 基于角色的访问控制

随着安全需求的发展，出现了第三种常见的访问控制类型，即基于角色的自主访问控制模型。这种机制在主体和访问权限之间引入了角色的概念，用户与特定的一个或多个角色向联系，角色与一个或多个访问权限相联系。这里所谓的角色就是一个或多个用户可执行的操作的集合，这体现了角色访问控制的基本思想，即通过用户在组织中担当的角色来授予用户相应的访问权限。举个例子，在一个公司中，董事长这个角色拥有其相应的权限。如果张三现在担任公司的董事长，那么张三就拥有董事长的权限对系统资源进行访问操作。如果在不久的将来，董事长换为李四来担任，那么李四就具有了董事长的权限，而张三就不在具有这样的权限了。

从上面的例子中可以看到基于角色访问控制的优势。那就是在系统发生变化时只需要修改主体与角色或角色与访问操作权限的对应关系就可以了，工作量大大减少。因此，这种方法经常用在组织中角色较多，且人事变动频繁的环境。

基于栅格的访问控制是非自主访问控制的变形。在这种访问控制中，主体和客体之间的每个关系都有一系列的访问边界。这些访问边界定义了允许访问客体的条件和规则。在大多数情况下，访问边界定义了符合安全等级和安全标签限制的最低限和最高限。

6.4 访问控制实现技术

访问控制的实现技术是指为了检测和防止系统中的未授权访问，对资源予以保护所采取的软硬件措施和一系列的管理措施等手段。实现访问控制的技术主要有 3 种。

1. 访问控制矩阵

访问控制矩阵是实现访问控制最初的概念模型。任何的访问控制策略最终均可被模型化为访问控制矩阵形式。在访问控制矩阵中，行对应访问主体，列对应客体资源，矩阵中的每个单元表明了主体对客体资源相应的访问权限。表 6-1 是一个访问控制矩阵的实例。

从下表中可以看出，主体 1 对客体 1 的访问权限为“拥有”、“读”、“写”。

但是，访问控制矩阵也存在着一定的缺陷。在实际组织中，由于主体对很多客体资源都不具有访问权限，必然导致矩阵过于稀疏，不利于实施访问控制。

表 6-1　访问控制矩阵实例

	客体 1	客体 2	客体 3	客体 4
主体 1	拥有		拥有	
	读			
	写		写	写
主体 2		拥有		拥有
	读	读		
主体 3			拥有	拥有
	读	读	读	读
	写		写	写

2. 访问控制表

访问控制表以客体资源为中心。在系统中，首先把客体排成一个表，然后在每个客体后面附加一个链表，表明哪些主体对此客体具有访问权限以及具有什么样的访问权限。图 6-2 是一个访问控制表的实例。

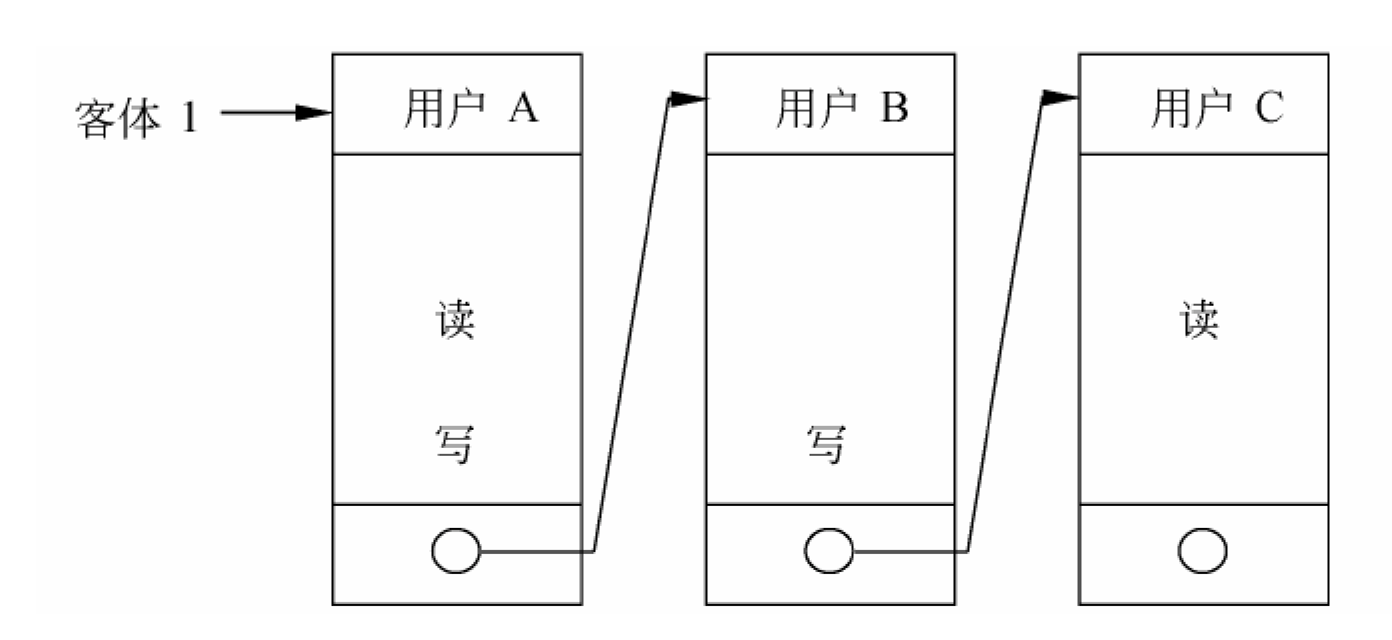


图 6-2　访问控制表实例

从图 6-2 中可以看出，用户 A、用户 B、用户 C 对客体 1 具有访问权限，其中用户 A 的访问权限为“读”和“写”，用户 B 的访问权限为“写”，用户 C 的访问权限为“读”。

3. 能力关系表

能力关系表以访问主体为中心。在系统中，首先把主体排成一个表，然后在每个主体后面附加一个链表，表明主体对哪些客体资源具有访问权限以及具有什么样的访问权限。图 6-3 是一个能力关系表的实例。

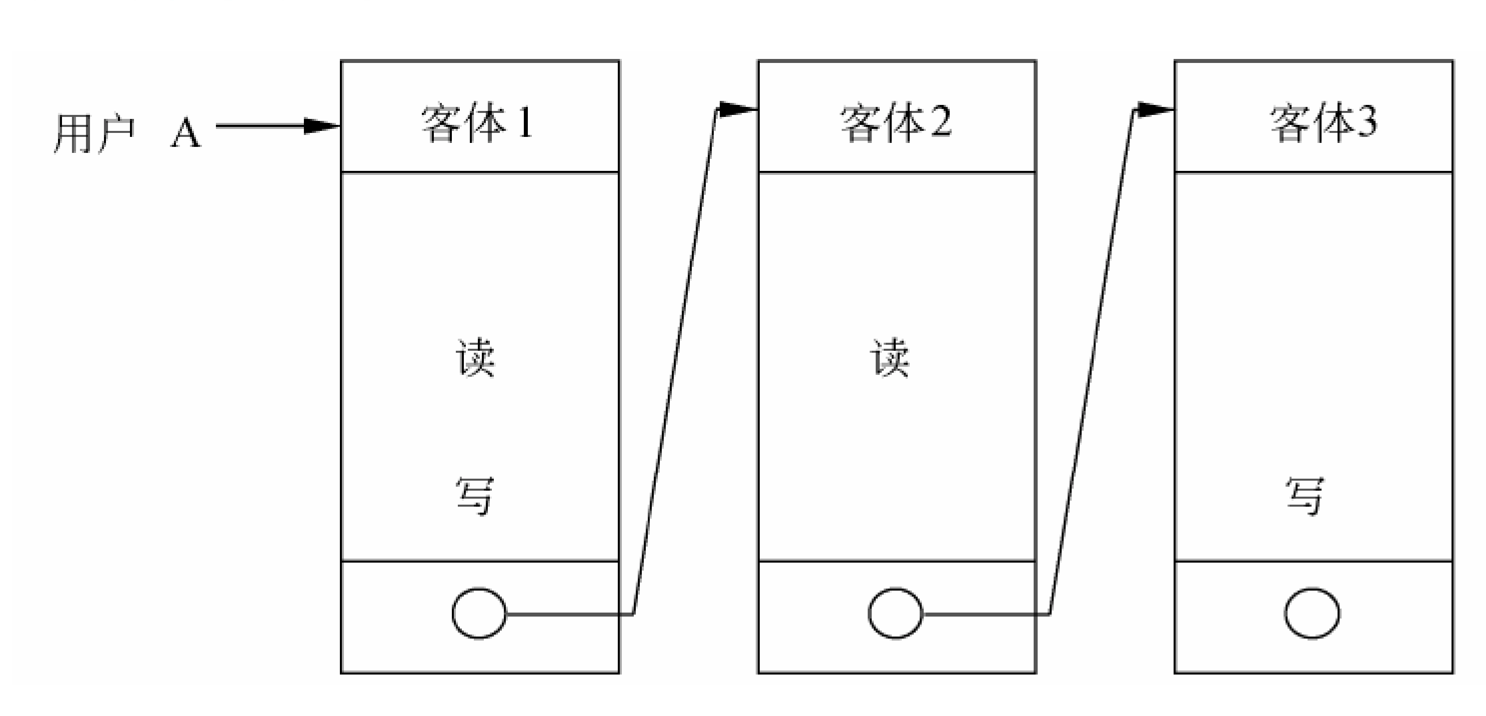


图 6-3　能力关系表

从图 6-3 中可以看出，用户 A 拥有对客体 1、客体 2、客体 3 的访问权限，对客体 1 的访问权限为“读”和“写”，对客体 2 的访问权限为“读”，对客体 3 的访问权限为“写”。

6.5 访问控制管理

访问控制管理可以同时使用集中式和分布式的方式来实施。最好的管理方式取决于系统需要以及存储于计算机系统中信息的敏感度。

1．集中式访问控制

集中式访问控制管理通过一个中心访问控制单元来处理系统所有的访问请求。由于只需要在一个地点进行对客体的管理，因此实施简单。但这种方法也存在着不容忽视的缺点。一方面，如果中心访问控制单元失效，那么所有的访问请求都得不到处理，进而造成所有的客体资源都不可用。另外，在系统访问请求较多的情况下，中心访问控制单元容易成为系统的瓶颈，影响系统的正常功能。

集中式访问控制的一个典型应用是 RADIUS 协议。在 RADIUS 服务器上，根据相应的方法对用户身份进行验证，然后根据系统的访问控制规则处理用户的访问请求。

2．分布式访问控制

分布式访问控制与集中式访问控制相反，系统中存在多个地点都可以对同一个客体资源进行管理。因此，这种方法更加稳定，不存在单点故障或者单点访问问题。然而，这种方法实现更加复杂，工作量更大。通常分布式访问控制使用安全域来实施。一个安全域指的是一个信任的范围或一些主体和客体，加上一些事先定义的访问规则和权限。一个主体必须包含在可信域中才能访问客体。这种方法使排除一个不可信的主体变得更加容易，但是由于安全规则精细粒度的增加使得管理变得更难。

6.6 访问控制模型

访问控制模型给出了系统安全策略概念化的视图。它可以把安全策略的目标、命令映射到特殊的系统事件上。这种映射过程考虑到了安全控制的形式化定义和详细说明。总之，访问控制模型把复杂的策略分解为一系列易管理的步骤。近些年，已经开发出多种不同的访问控制模型。一般而言，大多数完整的安全策略应用都会使用多种访问控制模型。

6.6.1 状态机模型

状态机模型是一系列状态以及特定状态转移的组合。当客体的状态发生变化的时候，就会在两个状态之间发生状态转移。状态机模型通常用来模拟现实的实体以及实体之间状态的转移。当一个主体请求访问某个客体时，必须有一个事先定义的允许客体从关闭

的不可读状态，变为开放状态的转移函数。图 6-4 给出了一个简单状态机的图示。状态用圆圈来代表，转移函数用箭头来代表。

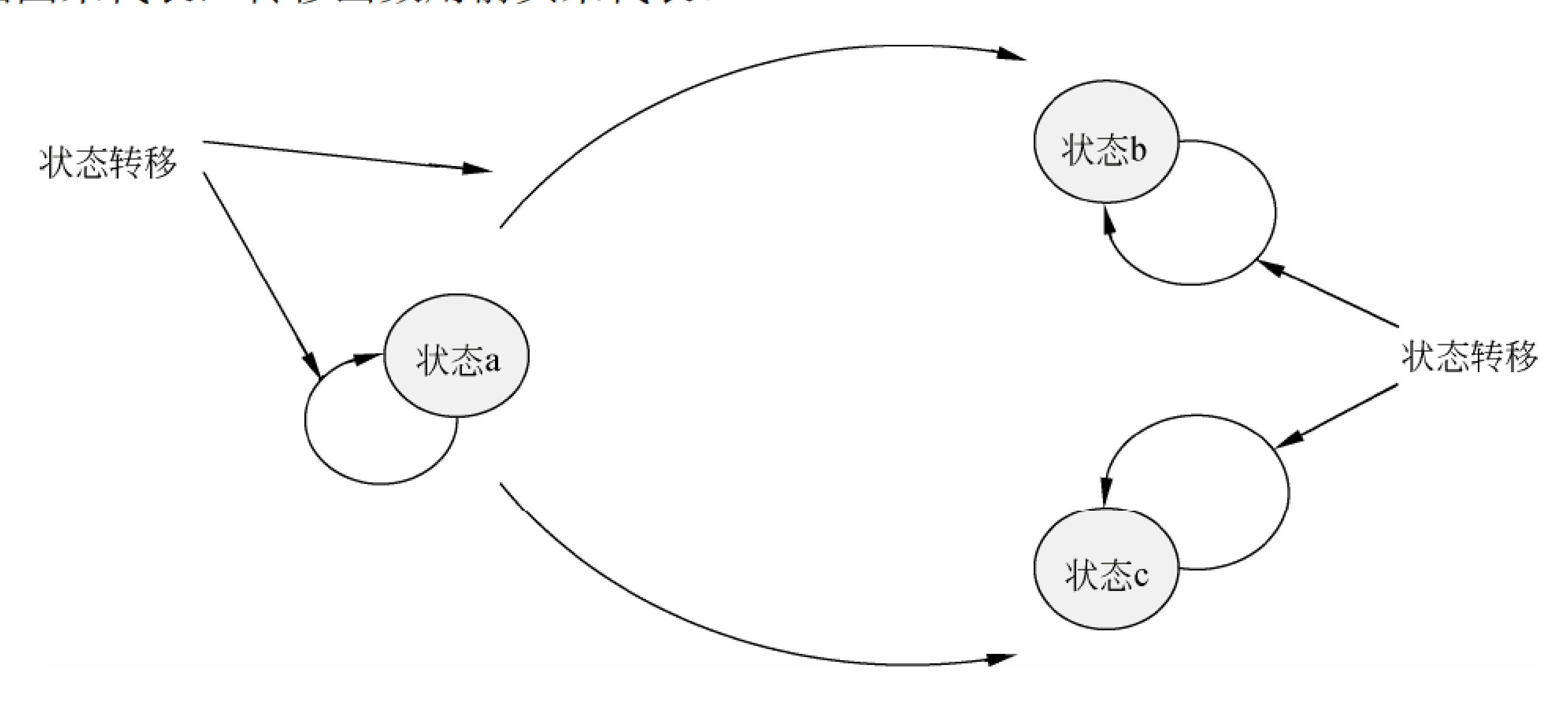


图 6-4　状态机模型

6.6.2　Bell-LaPadula 模型

Bell-LaPadula 模型开发于 20 世纪 70 年代，使用访问控制表和安全标签实现客体安全性，是典型的保密型多级安全模型。在早期的安全模型中，只要主体的安全级别高于客体的安全级别，就可以对客体进行访问。这样很容易造成信息的泄露，即高安全级别的主机将敏感信息写入较低安全级别的客体中，而较低安全级别的主体通过读操作就可以获得这些信息。

Bell-LaPadula 模型很好地避免了这一点。其基本思想是“无上读，无下写”。也就是只有当主体的安全级别高于客体的安全级别时，才能对客体进行读操作；只有当主体的安全级别低于客体的安全级别时，才能对客体进行写操作。表 6-2 给出了 Bell-LaPadula 模型的控制原则。这种方法有效避免了信息流向更低的安全级别流出，实现了信息的保密性保护，被广泛运用到需要对信息进行严格保密的环境。

表 6-2　Bell-LaPadula 模型

访问控制原则	通用名字	描述
简单安全规则	无上读	给定安全级别的主体不能读取安全级别更高的客体的数据
* 安全规则	无下写	给定安全级别的主体不能向安全级别更低的客体写入数据

6.6.3　Biba 模型

Bell-LaPadula 模型很好地解决了信息的保密性问题，但也同时存在着低安全级别的用户可以对高安全级别的用户数据进行修改、删除等操作，给信息的完整性带来威胁。

Biba 模型的开发正是为了实现对信息的完整性保护。

Biba 模型的基本思想是“无下读，无上写”。也就是只有当主体的安全级别低于客体的安全级别时，才能对客体进行读操作；只有当主体的安全级别高于客体的安全级别时，才能对客体进行写操作。表 6-3 给出了基本 Biba 模型的控制原则。由于对信息完整性的保护，这种模型更加适用于银行、电信等商业领域。

表 6-3　Biba 模型

访问控制原则	通用名字	描述
简单安全规则	无下读	给定安全级别的主体不能读取安全级别更低的客体的数据
* 安全规则	无上写	给定安全级别的主体不能向安全级别更高的客体写入数据

6.6.4　Clark-Wilson 模型

Clark-Wilson 模型是在 Biba 模型之后开发出来的。与 Biba 模型和 Bell-LaPadula 模型不同的是，Clark-Wilson 模型并不是建立在状态机模型上的，而是采用一种不同的方法来保证数据的完整性。Clark-Wilson 模型通过少量关系紧密的访问控制程序来限制所有的访问控制。这种模型在访问程序中使用安全标签来保证对客体的访问，更适合于数据完整性更加重要的商业环境中。

为了更好的理解模型的访问路径，Clark-Wilson 模型定义几个必需的术语。

- **受控数据（CDI）** 系统中的受控数据。
- **非受控数据（UDI）** 系统不受控制的数据条目（例如，数据输入或输出）。
- **完整性验证过程（IVP）** 核查受控数据完整性的程序。
- **变换程序（TP）** 用来改变受控数据的有效状态。

Clark-Wilson 模型确保所有的非受控数据经过完整性验证过程的核实，然后经由变换程序提交给系统。所有对受控数据的修改都要经由 IVP 和 TP 来进行。

6.7　文件和数据所有权

文件和数据可能包含着重要的信息。这些重要的信息应该是保护的重点。可以通过为每一个重要的信息来设定不同的安全级别来保护其安全。每一个文件或数据单元，应该至少有 3 个责任方。不同的责任方有着不同的安全要求。最常见的是数据所有者、数据托管者和数据使用者。每一方拥有各自的责任来支持系统的安全策略。

1．数据所有者

数据所有者具有数据保护的最高责任。数据所有者通常是组织最高管理者，代表整个组织来行事。数据所有者设置数据的安全级别并且选择数据托管者来完成对数据的维护。如果发生安全事件，首先要追究数据所有者的责任。

2. 数据托管者

数据所有者指派数据托管者根据数据安全等级来确保安全策略。数据托管者通常是IT部门的成员，遵循明确的规程来保护数据，包括实施和维护合适的控制，设置备份，以及验证数据的完整性。

3. 数据使用者

数据的使用者是访问数据的用户。当他们访问数据的时候要遵循一定的安全策略，不仅要遵守安全规程，数据使用者还必须认识到安全规程对于组织安全的重要性。因为缺少对控制重要性的理解，用户常使用捷径绕过薄弱的安全控制。一个组织的安全工作者必须不断努力，使得数据使用者意识到安全以及安全策略、安全规程的重要性。

6.8 相关的攻击方法

实施访问控制最主要的目的是阻止对敏感数据的未授权访问。攻击者主要目的是访问这些敏感的数据。有几种和访问控制相关的攻击类型。最主要的类型是阻止访问控制或旁路访问，使得未授权的主体去访问客体。

1. 穷举攻击

穷举攻击就是尝试所有可能的字母组合来满足认证口令，以获取对客体的访问权限。在这种攻击中，使用口令猜测程序，不断向系统提出登录请求，并且在每一次请求时使用不同的口令，以求找到正确的口令。穷举攻击的一个变体是竞争拨号。这种攻击中，程序拨打大量的电话号码，监听调制解调器的应答。当竞争拨号程序发现了一个调制解调器做出了应答，这个号码就被记录下来用于攻击。

保护系统免受此类攻击的一个有效方法是主动在自己的系统上运行穷举攻击，以此找到系统破绽。首先确信系统已经许可执行这种攻击了。当使用这种手段来保护系统的时候，实际上已经破坏了安全策略。另外，只运行一次是不够的。一旦用户对记忆复杂的口令感到疲惫，或是发现使用口令来访问 Internet 很难的时候，就会使用简单口令以及未授权的调制解调器。因此，要定期运行穷举攻击来找到利用系统缺点的用户。

为了保护系统安全，还可以设置监控系统来监控系统不正常的行为，并及时发出警报。当然还可以设置停工阈值，使得用户在一定次数的登录失败之后，账户被锁定。尽管对于丢失口令的用户，这种方法有点令人沮丧，可是却能很好地对抗穷举攻击。

2. 字典攻击

字典攻击事实上就是穷举攻击的子集。字典攻击并不尝试所有的口令组合，而是从一个列表或字典中尝试那些常用的口令。很容易找到那些常用的用户ID和口令。抵抗字典攻击最好的方法就是使用较强的口令策略。口令策略告诉用户如何来生成一个口令，要避免什么样的口令。通过生成和加强一个安全性较高的口令策略，可以避免口令出现在口令字典中。一旦选择了口令，要定期使用字典攻击来检测口令的安全性。这些攻击

不像穷举攻击那样集中，能够使人清楚地认识到系统中的哪些用户遵守着口令策略。避免以明文的形式发送口令同样可以防止口令的泄露，基于这个原因，要避免使用 HTTP 和 Telnet。当需要向一个网站发送口令的时候，使用另一种协议，例如 HTTP-S。

3. 欺骗攻击

另一种针对访问控制的攻击类型是欺骗攻击。攻击者放置一个伪造的登录程序来迷惑用户，骗取用户 ID 和口令。这种方式看起来就像是正常的登录屏幕，所以用户很可能提供需要的信息。程序并不会把用户连接到所请求的系统上，而是返回一个登录失败的提示信息。事实上，程序已经存储或者是转发了偷来的用户认证信息。接下来才会出现真正的登录屏幕。这种方法的高明之处在于当用户面前出现一个登录失败的屏幕时，很少有人会想到这是一个欺骗攻击。

抵御这种攻击最好的方法是在用户和服务器之间创造一个可信路径，来减少攻击者在用户和服务器之间介入的机会。在对安全要求极高的环境中，用户应该检查所有失败的登录请求，确保所有的失败都进行了合适的记录和报告。对于阻止和检测这些类型的攻击，安全意识在此起到了很重要的作用。

习　　题

一、选择题

1. 以下哪一项不是通过实施访问控制来阻止对敏感客体进行未授权访问攻击？（　　）

   A. 欺骗攻击
   B. 暴力攻击
   C. 穷举攻击
   D. 字典攻击

2. 以下哪个模型通常用来模拟现实的实体以及实体之间状态的转移？（　　）

   A. 状态机模型
   B. Bell-LaPadula 模型
   C. Clark-Wilson 模型
   D. Noninterference 模型

二、简答题

1. 什么是访问控制，其一般过程是什么？
2. 列举常见的访问控制模型，并说明其原理。
3. 访问控制中都有哪些常用的攻击方法，其原理是什么？

课后实践与思考

1. 举例说明在工作中所遇到的攻击方法，并说明其原理。
2. 说明您所在的单位是如何应付各类访问控制攻击的？

第 7 章　防火墙技术

本章学习重点：

- 解释路由器、代理服务器和防火墙为计算机网络提供的边界保护
- 描述防火墙 3 种主要的拓扑结构（堡垒主机、屏蔽子网、双重防火墙）
- 如何在不同的环境内设置合适的防火墙
- 设计满足组织工作需要和安全需求的防火墙过滤规则库
- 解释在构建防火墙规则库的过程中，清除规则和隐形规则的重要性

计算机安全、物理安全、数据安全等各种领域都认识到边界安全的重要性。网络安全的基本责任就是保护网络的边界安全，防止恶意活动的破坏。

本章的重点就是保护网络边界安全技术的应用。读者将会了解到如何使用路由器、代理服务器以及防火墙等设备建立一个抵抗恶意攻击行为的防护系统；同时介绍虚拟专用网如何使在保护边界之外的用户获得使用网络内资源的能力。

7.1 边界安全设备

网络设备构成了网络边界安全的核心。大多数的信息安全从业者在业务需求、经济条件、技术条件以及有限的人力资源的限制下，共同使用包括路由器、代理网关以及防火墙在内的各种设备来构建、维持和检测网络边界，达到尽可能高的防护水平。

需要注意，在构建网络边界的时候一定要构建一个可被管理的防御体系。如果组织内的人员只够用来有效地管理和检测少量安全设备，那么最好的选择是构建一个有限系统，而不是建设一个不能控制的大规模的系统。实际上，一个设置不合理的网络安全设备很可能会形成网络的一个威胁，破坏整个网络的安全。

在这一部分，读者将会看到在网络边界保护中使用的 3 种主要安全设备。这些设备用来加强访问控制，防止恶意活动破坏网络。保护网络的另外一个重要组成部分是使用入侵检测系统来检查对网络边界的成功渗透。

7.1.1 路由器

路由器的一个重要作用是连接网络，并且给发往目的地的通信流量选择合适的路由。在保护网络的边界安全中，路由器同样起到了很重要的作用。大多数情况下，路由器是用户从因特网进入网络所碰到的第一个物理设备。因此，路由器应该限制进入被保护网络的通信流量，以此来加强网络安全。

路由器确实包含一些安全功能。例如，思科路由器可以通过为不同的传输协议和网络协议定制不同的访问控制链表（ACLs）来实现相对复杂的包过滤。路由器同样可以减少其他边界安全设备上的负载，保护这些设备免受拒绝服务攻击。例如，一个试图攻破

防火墙的恶意攻击者可能会使用网络流量或向这个防火墙发送大量精心制造的数据包来淹没这个防火墙。在大多数情况下，因特网和防火墙之间有一个路由器。如果安全管理员能够设置这个路由器使它拒绝这种以防火墙为目标的数据包，这种攻击就能够被制止。

路由器同样可以阻止对一个网络的欺骗攻击。在这种攻击方式中，恶意攻击者试图把自己伪装成网络的内部人员，以此来获得对一个网络的越权访问。攻击者使用的最常见的一种方法是改变 IP 地址，这样看起来似乎就是一个在目标网络内部的地址。路由器通过检查一个去往目标网络的数据包的包头，就能够很容易地检查出这种类型的攻击。例如，考虑图 7-1 给出的情况，在这种情况下，路由器保护着北京网络，这个网络的专有 IP 地址是 123.116.0.0。它把这个网络和上海网络（这个网络的专用 IP 地址段是 114.80.0.0）通过一个专线连接在一起。同时，它还维持着北京办公室和互联网之间的连接。

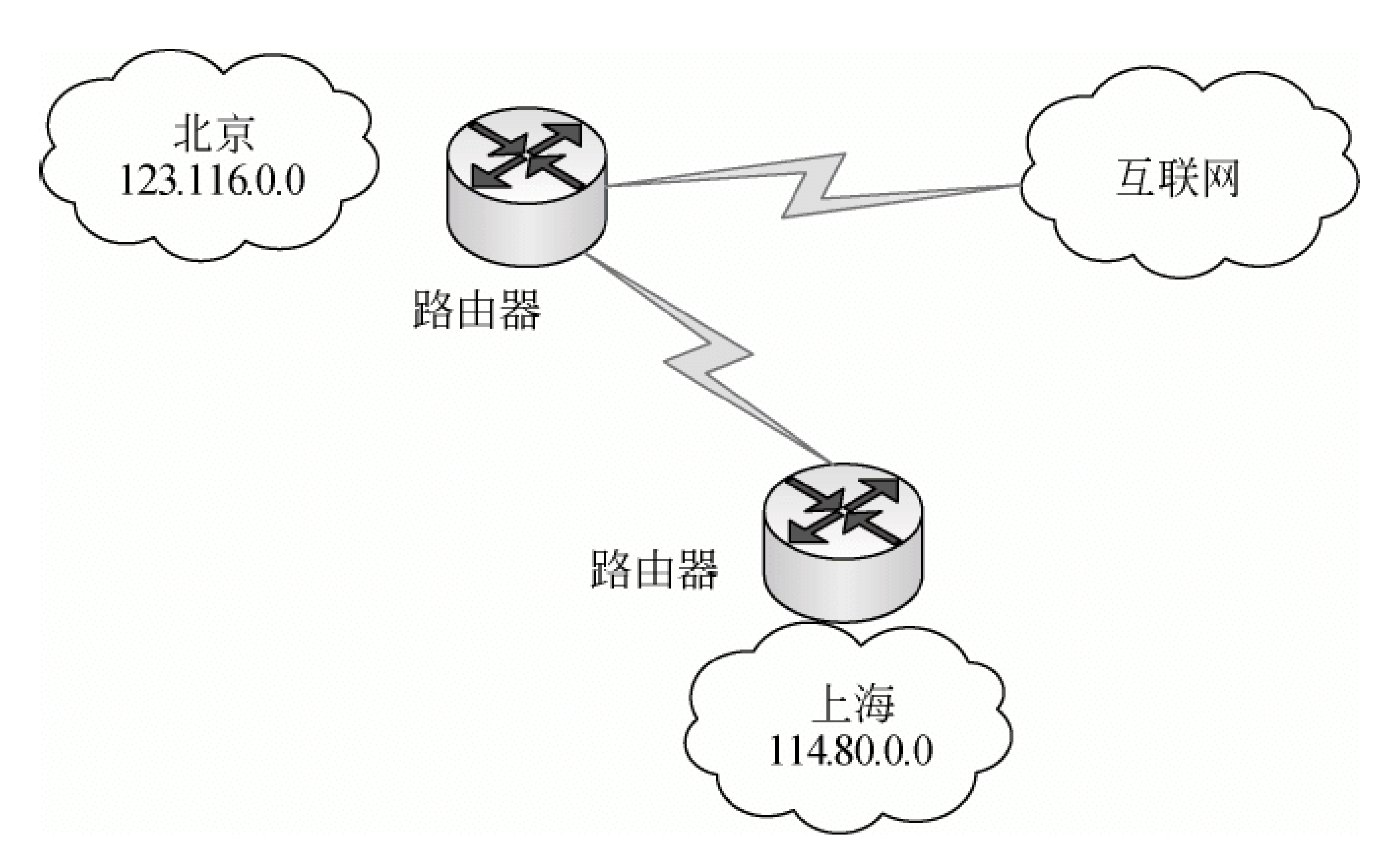


图 7-1　路由器保护网络示意图

一个试图阻止欺骗攻击的管理员会考虑到两种情况。首先，要保证来自于外部连接的具有 123.116.0.0 地址段 IP 地址的通信流量不能进入被保护的网络。任何这样的数据包几乎就是恶意攻击或错误系统配置的标志。第二，管理者应该对这个路由器进行设置使其拒绝任何来自于因特网但是源地址是 114.80.0.0 网段的数据包。任何来自于上海网络的合法通信数据包应该通过特定的网络连接。如果一个具有上海 IP 地址的数据包出现在路由器因特网的接口上，这很可能同样是错误网络配置或恶意攻击的标志。

另外，用户除了要保护自己的网络免受欺骗攻击，同样还应该采取措施来保证自己的网络没有被用来作为欺骗攻击的发射点，这可以通过使用出站过滤来实现。当实施出站过滤时，用户路由器除了要检查进入网络的数据包，还要检查离开网络的数据包。要确保离开用户网络的数据包拥有一个来自于此网络的合法 IP 地址。在图 7-1 中，任何通过这个路由器离开北京网络的数据包都要拥有一个 123.116 地址段的合法 IP 地址。如果不是这样的话，说明黑客可能正在利用此网络发射一个针对外部网络的攻击。这种情况同样意味着用户的网络上可能出现越权系统或错误设置的系统。

7.1.2　代理服务器

在政府、法律和商业应用中，代理指被授权代表一个人或组织行事的另外的一个人

或组织。在计算机网络中，代理服务器以类似的方式工作。计算机工作中最不安全的情况是位于受保护的内网中的客户端想要访问位于不可信系统中的资源。在这种情形下，不可信系统可能执行一系列非法活动，举例如下。

（1）向客户端系统传递恶意代码并私自运行。

（2）获取客户端系统的真实 IP 地址。

（3）识别客户端系统运行的软件类型，查找软件所具有的潜在漏洞。

图 7-2 给出了这种典型的客户/服务器的相互作用方式。

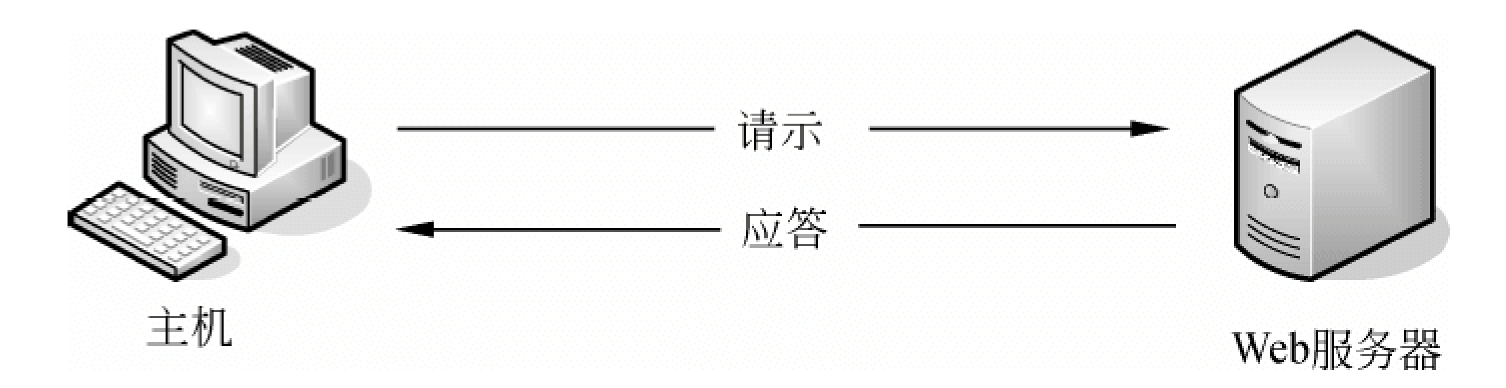


图 7-2　客户/服务器作用方式

通常，当网络中存在代理服务器时，客户端就不会直接访问因特网主机。相反地，它们的请求被转发给代理服务器，接下来由代理服务器分析这个请求，然后决定该请求是否是可允许的。如果这个请求通过了批准，代理服务器会使用下面的步骤来实现这个请求。

（1）代理服务器首先检查自己的数据缓冲区，确认在之前它是否为客户端回答过相同的请求。

（2）如果服务器缓存中有这些信息，那么服务器考虑这些信息是否足够用来回答客户端的这个请求。这个过程可以通过对数据上的时间戳和一个可设置的阀值进行比较来完成。如果目前这些信息是足够的，那么代理服务器就使用缓存中的信息来回答客户端的请求，过程结束。

（3）如果缓存中的信息已经过时了或在缓存中并不存在被请求的信息，那么，代理服务器就会代表客户端向远程的 Web 服务器发起一个请求。这个 Web 服务器并不知道代理服务器的存在，它只是把代理服务器当成和其他客户端一样的客户端。接下来，它会把应答数据发送给代理服务器。

（4）当代理服务器收到来自于 Web 服务器的信息时，它会首先处理这个应答信息（因为这个信息中有可能包含恶意内容），然后应答客户端的请求。

（5）如果这个服务器使用了缓存，接下来，它会在缓存中存储应答信息的副本，这样就能方便之后应答来自网络客户户的请求。

图 7-3 给出了客户端/代理服务器/服务器之间的相互交互过程。

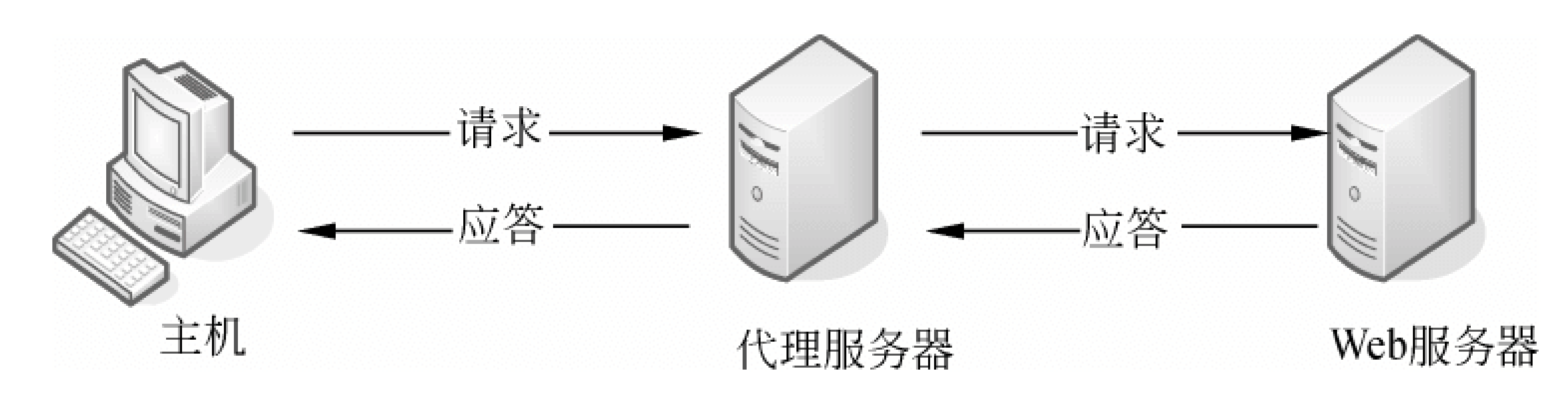


图 7-3　客户/代理服务器/服务器作用方式

从安全的角度讲，代理服务器隐藏了网络上客户端的身份，限制了网络嗅探的有效性。同时，代理服务器使得安全管理者能够执行许可使用策略（通过限制用户请求内容的种类），并且能够过滤输入数据的恶意内容，从而提供了过滤功能。从性能的角度讲，代理服务器并没有为每一个请求都建立一个因特网通信连接，而是经常从服务器的缓存中提供请求的信息，因此优化了使用带宽。

7.1.3 防火墙

防火墙负责过滤进入或离开计算机网络的通信数据，通过对接收到的数据包和防火墙内部过滤规则库中的安全规则进行比较，决定是否把一个数据包转发到它的目的地。

防火墙通常被视为网络安全的“银子弹”。确实，它们给一个未受保护的网络提供了极大的好处，并且能够独立地改善这个网络的安全状况。然而，防火墙并不是网络安全的灵丹妙药，它们的效益必须在一定的条件下才能够实现。在网络安全中，防火墙起到了很重要的作用，但是，它们仅是复杂的边界保护链中的一环。

7.2 防火墙的种类

防火墙成为计算机安全科学的一部分已经有很长一段时间了。在过去的这些年中，随着因特网技术的不断向前发展以及网络管理者注意力向着安全问题的转移，防火墙技术也在不断地进化。在现在的市场上，可以看到不同种类的防火墙解决方案和技术手段。这一部分，读者将会看到软件和硬件防火墙之间的不同，以及两种最普遍的防火墙过滤技术：包过滤和状态检测。

7.2.1 硬件防火墙和软件防火墙

当选择防火墙解决方案时，通常有两种选择平台：基于硬件的防火墙和基于软件的防火墙。基于硬件的防火墙（通常是指“电器用具”）是一种包含了运行防火墙所必需的所有硬件和软件的整合方案。它们是一种独立的设备，向管理者提供了防火墙安全的一种特定的解决方案。从管理者的角度来看，无论看起来还是感觉起来，基于硬件的防火墙和基于软件的防火墙都是很类似的，它们都使用了同样的图形化用户接口，同样的日志/审计功能，同样的远程配置功能。然而，作为一个专用的应用工具，比起基于软件的防火墙，基于硬件的防火墙处理数据的速度更快，更适用于高带宽的环境。当然，这种额外的性能来自于相对更高的价格。购买一个防火墙比自己使用一些独立的构件组建和配置一个防火墙似乎更昂贵一些。

基于软件的防火墙是安装在 PC 平台上的软件产品，通过在操作系统底层工作来实现网络管理和防御功能，相对硬件防火墙要更便宜一些。当用户购买了一个防火墙软件许可协议之后，就得到了一个可以安装在任何支持平台上的介质，可以用来安装和配置一个防火墙。大多数的商业防火墙适用于 Windows、Linux 以及 UNIX 的各种版本。如果用户从中间商手中购买自己的系统，那么一般而言，这个价格中就会包括设计防火墙

过滤规则库，设置系统以及对系统持续的维护和支持的费用。尽管安装和设置防火墙不是非常复杂，可是除非组织中有拥有防火墙经验的人员，否则使用这种支持是一种明智的选择。在配置防火墙过程中的一点小的失误可能会导致用户失去使用防火墙可能获得的全部好处。

7.2.2 包过滤防火墙

最早期的防火墙使用包过滤的原则来检查通过一个网络的通信。在这种方法中，每一个入网的（或出网的）数据包被单独处理。防火墙读取包头，分析包含在其中的路由和协议信息。大多数防火墙对于要分析的域不尽相同，但是最主要的包括源地址、目标地址、目的端口和传输协议 4 种。

很多的包过滤方案允许考虑其他的因素来做出决定，这些因素包括星期几或某一天的具体时间。例如，用户希望只有在非工作时间，网络使用率较低的时候，允许一定种类的非工作信息数据包通过防火墙。这些功能使得防火墙除了是一个边界安全工具，还可以称为性能优化工具。

7.2.3 状态检测防火墙

包过滤防火墙的一个主要缺点是单独分析每一个数据包，但是不能维持状态信息的连接。下一代防火墙技术——状态检测防火墙克服了这一缺点。状态检测防火墙维持了关于连接开放的数据以确保数据包是一个由合法用户建立的连接的一部分。

最简单的理解状态检测防火墙的方法就是通过例子。当客户端向一个远程服务器请求一个 Web 网页时两台电脑的工作过程如下。

（1）客户端使用一个随机高编号的端口（假设这个端口是 142 3 ）向目的主机的 80 端　口发送一个请求。

（2）目的服务器接受这个连接请求，并用一个随机选择的高编号端口（假设是 2901）来应答客户端上的 1423 端口。

（3）接下来，客户端的 1423 端口和服务器的 2901 端口进行通信。

这个精心设计的过程是为了保证知名端口（在例子中是 80 端口）能够及时应答服务连接请求。然而，这样做却给防火墙管理者制造了一个麻烦。如果仅使用包过滤防火墙，必需开放高编号的端口来适应这种情况。不幸的是，允许远程系统使用这些开放的高编号端口和受保护的网络进行连接是有很大风险的。

状态检测防火墙包含先进的技术，能够跟踪连接的状态。当客户端发出一个连接建立请求时（由防火墙的过滤规则库决定是否允许建立这个请求），防火墙积极侦听应答信息，并且记录正在被客户端和防火墙使用的两个端口。在连接存在的整个时期，来自这些端口的数据包被允许通过防火墙。当防火墙观察到连接拆除中的 FIN-FIN/ACK-ACK 标志时，它就会撤销临时授权，在这两个套接字中的通信就被阻断了。当一个连接的时间超出指定的阀值时，也会发生同样的动作。

7.3 防火墙拓扑结构

为了更加高效，防火墙必需被合理配置在一个网络上。防火墙应该被放在被保护网络和由外部访问此网络的所有路径之间。另外，许多组织选择使用内部防火墙来分割网络，使其在地理上或在功能上得到更进一步的保护。

本章将要讨论 3 种常见类型的防火墙拓扑结构。值得注意的是，这些方案用来保护整个网络免受来自于外部的攻击。还有很多把这些基本的方案进行混合搭配的更为复杂的拓扑结构，用来提供内部网络的分层保护。

7.3.1 屏蔽主机

屏蔽主机拓扑结构，如图 7-4 所示，防火墙是连接内网和外部网络的唯一链路。所有进入或离开内网的数据包都必须经过这个防火墙。这种拓扑是最容易应用的，也是最便宜的。然而，如果内网向外网提供某种服务，这种结构同样面临着巨大的安全风险。

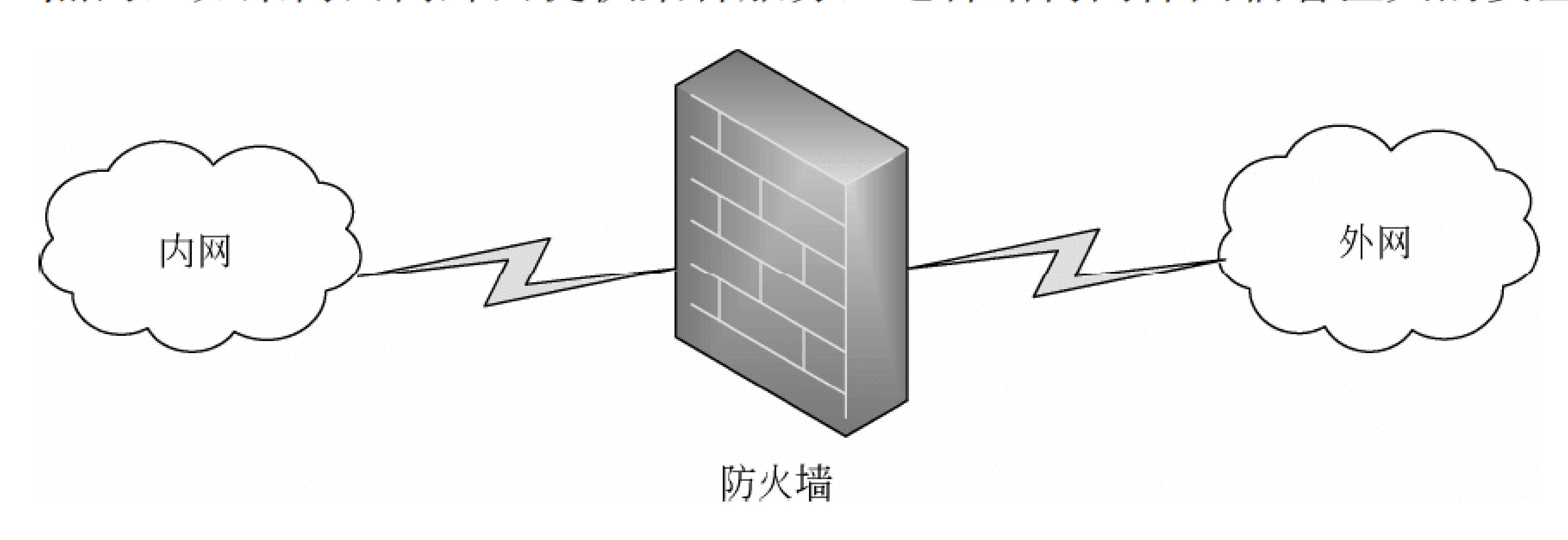


图 7-4 屏蔽主机结构

例如，假设在内网中包含一个旨在向因特网用户提供服务的 Web 服务器，为了提供这种服务，屏蔽主机的防火墙必须允许所有来自于因特网主机而指向 Web 服务器 80 端口的数据包通过。因此，如果恶意用户对 Web 服务器的攻击数据包使用 80 端口，也能通过防火墙。一旦 Web 服务器被攻破，攻击者就可以不受限制地访问内部网络资源了，这显然是极其危险的。下面两种防火墙拓扑结构就做出了一定的改变来减少这种威胁的风险。

7.3.2 屏蔽子网防火墙

屏蔽子网（通常被称为非军事区或 DMZ）防火墙拓扑结构同样是使用一个防火墙，但是，有 3 个网络接口。对于堡垒主机防火墙，一块网卡连接因特网（或其他外部网络），另一个连接内网。对于屏蔽子网防火墙，第三块网卡连接屏蔽子网，如图 7-5 所示。

屏蔽子网的目的就是提供一个中间地带作为因特网和内网之间的中立地域（因此叫做非军事区 DMZ）。管理员把向外部用户提供服务的系统放在这个网络上，例如 Web 服务器、SMTP 服务器等。以这种方式，即使一个恶意攻击者能够攻陷向公众提供服务的

服务器，也只是获得了对网络剩余部分有限的访问。攻击者可能会获得设置在 DMZ 区域上的系统访问权，但是获得内网访问权的机会却大大降低了（假设防火墙和过滤规则库设置是正确的）。

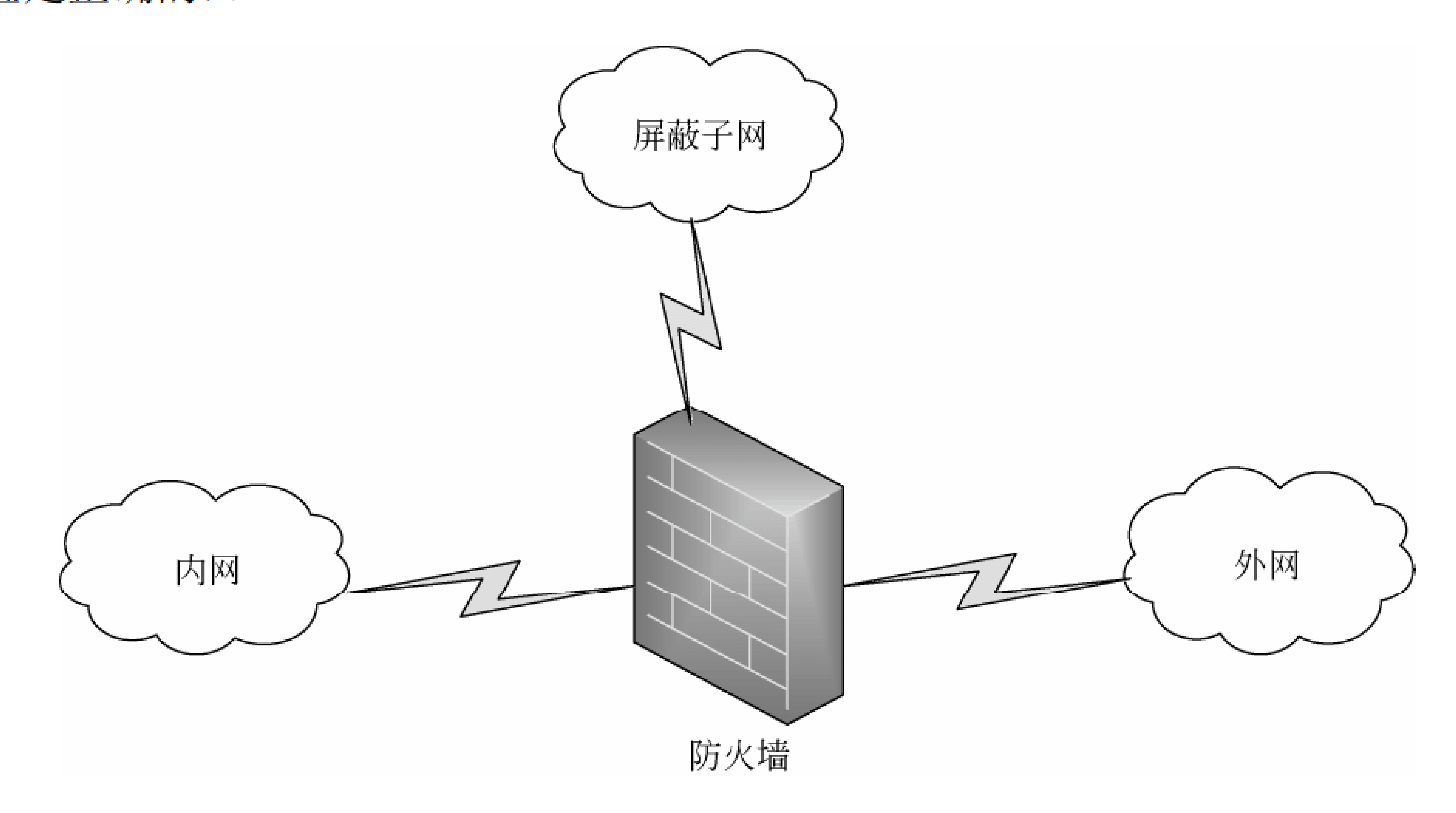


图 7-5 屏蔽子网结构

7.3.3 双重防火墙

最后一种防火墙拓扑结构是双重防火墙，如图 7-6 所示。像屏蔽子网防火墙一样，双重防火墙同样提供一个 DMZ 网络用来设置公共服务。然而，双重防火墙并没有使用一个带有 3 块网卡的防火墙来实现这个目标，而是使用两个带有两块网卡的防火墙来创建一个中间区域。

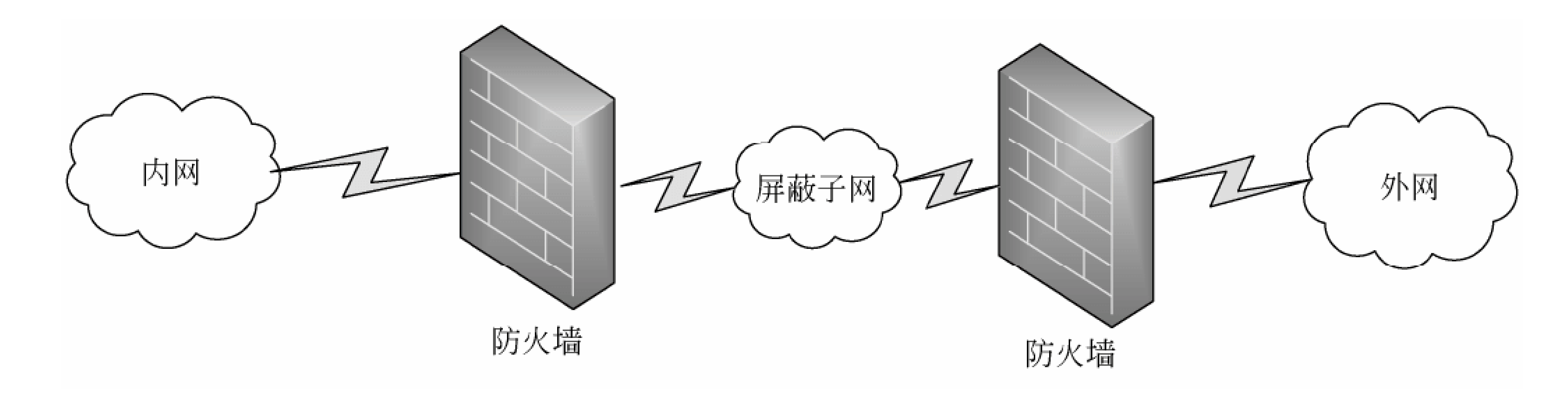


图 7-6 双重防火墙结构

双重防火墙除了提供和基本的屏蔽子网防火墙一样的安全效益，还提供了另外的好处。使用两个单独的防火墙使恶意攻击者攻破防火墙的可能性降到了最低。这种拓扑结构最有效的变体是在应用中使用两个本质上根本不相同的防火墙。为了实现这种变异，用户可以使用下列方法。

（1）一个系统使用硬件防火墙，另一个系统使用软件防火墙。

（2）使用来自不同供应商的防火墙。

（3）使用拥有不同安全认证标准的防火墙。

通过这种差异获得的最主要的好处是不同的防火墙具有同样内部漏洞的可能性是很低的。需要注意，防火墙和其他的计算机系统是基于同样类型的硬件和软件的。因此，也一定会有很多未被发现的安全漏洞。但是，当这些漏洞被发现的时候，防火墙供销商总是很快地发布这些安全补丁。使用双重防火墙提供了安全保护的附加层，成为阻止攻击者成功渗透到内部网络的屏障。

7.4 防火墙过滤规则库

7.4.1 概述

防火墙的过滤规则库是边界安全架构中最为重要的组成部分。这个规则库规定了网络上的哪些数据包可以通过，哪些数据包应当被阻塞。防火墙的管理者应该花费大量的时间来进行防火墙过滤规则库的设计、配置、维护和更新。

每一个防火墙使用不同的语法方式对规则进行说明，大多数提供一个图形化的用户接口使得规则的输入变得很容易。然而，在不同的平台上，基本的功能是不变的。大多数的规则具有下面的形式：


```
<action> <protocol> from <source_address> <source_port> to
<destination_address> <destination_port>
```

这些域至少包含下面这些值。

（1）<action>的值是 deny 或 allow。

（2）<protocol>的值是 tcp、udp、或 icmp。

（3）<source_address>和<destination_address>的值可能是一个 IP 地址，也可能是一个 IP 地址范围或“any”关键字。

（4）<source_port>和<destination_port>的值可能是端口号或“any”关键字。

正如之前所讲的，这只是所有防火墙支持的基本功能。大多数系统使用一些更高级的应用，使得管理员能够按照组织业务的需求设置防火墙的功能。这类功能包括以下 4 种。

（1）终止（而不是阻塞）入站的数据包。被终止的数据包仅是被忽略了，相反，当数据包被阻塞的时候会通知通信的发起者。

（2）整合防火墙自身（外部的）的认证系统来向不同的级别的用户提供不同的安全限制。

（3）与虚拟专用网方法相结合。

（4）设置服务质量的规则，使得一定类型的网络流量事先排好序。

设计防火墙规则库的时候，首先要列出由这个网络所支持的业务要求，然后找出为了完成这些业务要求所必须实现的服务，最后创建能够实现这些特定服务的防火墙规则列表。安全管理员最常见的错误是开始时先列出防火墙支持的规则，然后再来找相应的

业务需求。这样做会造成两个问题：首先，业务需求有可能被忽视，从而导致规则库的重建；另外，这种方法有可能会导致管理员扩充业务要求来适应目前可被允许的服务。

7.4.2 特殊规则

有两个特殊的规则应该被放在每一个防火墙规则库中：清除规则和隐形规则。这些规则是组织的基本安全原则。

1. 清除规则

清除规则完成了防火墙最基本的功能：拒绝不被明确允许的任何东西。在本章使用的语法形式中，这将会被写成如下的形式：

```
deny any from any to any any
```

因为这种语法形式，清除规则又被称为“deny any”规则。在每一个防火墙规则库中这应该是最后一个规则。如果为了实现某个安全目标而必须撤出这个规则，那么防火墙的这种过滤规则库设计的是不够好的，需要重建。

2. 隐形规则

隐形原则是为了保护防火墙本身免受来自外部（内部）的攻击，阻止网络上对防火墙的任何形式的直接连接，限制访问那些和网络有物理连接的用户。这个规则可以被写成下面的形式：

```
deny any from any any to firewall any
```

这里，firewall 指的是防火墙本身的 IP 地址。

在所有防火墙的规则库中，隐形规则应该是第一规则。然而，有些情况下，用户可能希望允许某些到防火墙的受限连接。在这种情况下，第一规则应该明确允许这些连接，然后紧跟着是隐形规则。

习　　题

一、选择题

1. 以下哪一项不是通过实施访问控制来阻止对敏感客体进行未授权访问攻击的？（　　）

A. 欺骗攻击

B. 暴力攻击

C. 穷举攻击

D. 字典攻击

2. 常见类型的防火墙拓扑结构不包括以下哪一项？（　　）

A. 屏蔽主机防火墙

B. 屏蔽子网防火墙

C. 双重防火墙

D. 硬件防火墙

二、问答题

1. 试说明在保护网络的边界安全中路由器所起的作用。

2. 简述客户端/代理服务器/服务器之间的相互交互过程。

3. 举例说明常见的防火墙类型。

4. 常见的防火墙拓扑结构有哪些?简单说　　明其原理。

课后实践与思考

网络卫士防火墙配置实例

实例 1：路由模式下通过专线访问外网

路由模式下通过专线访问外网，主要描述总公司接入网络卫士防火墙后的简单配置，总公司的网络卫士防火墙工作在路由模式下，如图 7-7 所示。（提示：用 LAN 或者 WAN 表示方式。一般来说，WAN 为外网接口，LAN 为内网接口。）

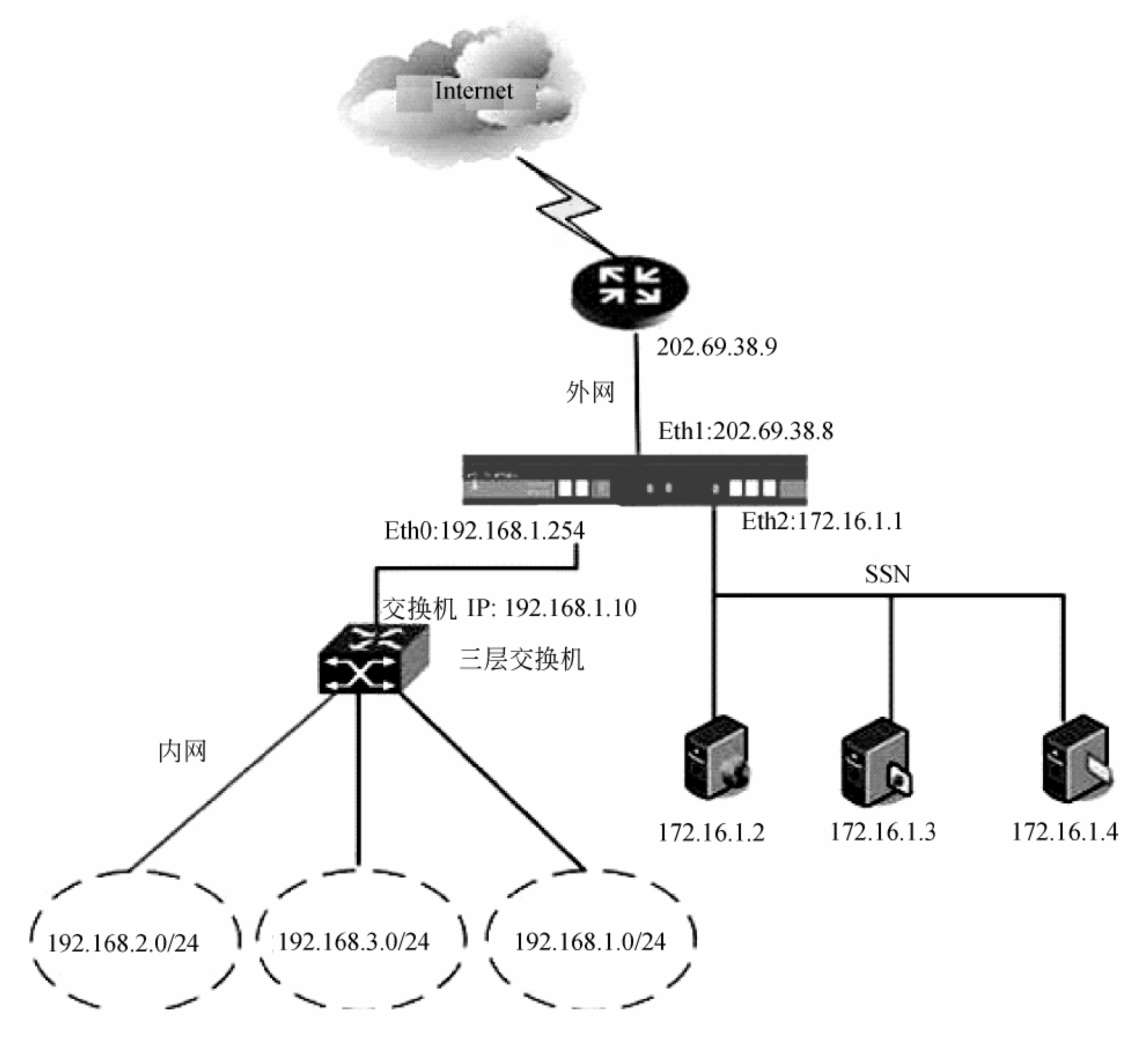


图 7-7　网络卫士防火墙的路由模式

1．网络状况

（1）总公司的网络卫士防火墙工作在路由模式下。Eth1 属于外网区域，IP 为 202.69.38.8；Eth2 属于 SSN 区域，IP 为 172.16.1.1；Eth0 属于内网区域，IP 为 192.168.1.254。

（2）网络划分为 3 个区域：外网、内网和 SSN。管理员位于内网中。内网中存在 3 个子网，分别为 192.168.1.0/24，192.168.2.0/24，192.168.3.0/24。

（3）在 SSN 中有 3 台服务器：一台是 HTTP 服务器（IP 地址：172.16.1.2），一台是 FTP 服务器（IP 地址：172.16.1.3），一台是邮件服务器（IP 地址：172.16.1.4）。

2．用户需求

（1）内网的机器可以任意访问外网，也可访问 SSN 中的 HTTP 服务器、邮件服务器和 FTP 服务器。

（2）外网和 SSN 的机器不能访问内网。

（3）允许外网主机访问 SSN 的 HTTP 服务器。

3．配置步骤

（1）为网络卫士防火墙的物理接口配置 IP 地址。

进入 NETWORK 组件 topsec# network

配置 Eth0 接口 IP topsec.network# interface eth0 ip add 192.168.1.254mask255.255.255.0

配置 Eth1 接口 IP topsec.network# interface eth1 ip add 202.69.38.8 mask255.255.255.0

配置 Eth2 接口 IP topsec.network# interface eth2 ip add 172.16.1.1 mask255.255.255.0

（2）内网中管理员通过浏览器登录网络卫士防火墙，为区域资源绑定属性，设置权限。

设置内网绑定属性为“Eth0”，权限选择为禁止。

设置外网绑定属性为“Eth1”，权限选择为允许。

设置 SSN 绑定属性为“Eth2”，权限选择为禁止。

（3）定义地址资源。

定义 HTTP 服务器：主机名称设为 HTTP_SERVER， IP 为 172.16.1.2。

定义 FTP 服务器：主机名称设为 FTP_SERVER， IP 为 172.16.1.3。

定义邮件服务器：主机名称设为 MAIL_SERVER， IP 为 172.16.1.4。

定义虚拟 HTTP 服务器：主机名称设为 V_SERVER，IP 为 202.69.38.10。

（4）定义地址转换规则，见表 7-1。

表 7-1　地址转换规则

内网用户通过源地址转换访问外网	转换控制选择“源转换”； 源区域选择“内网”； 目的区域选择“外网”； 服务不选，表示全部服务； 源地址转换为“eth1”
外网用户通过目的地址转换访问 HTTP 服务器	转换控制选择“目的转换”； 源区域选择“外网”； 目的区域选择“SSN”，目的地址选择“V_SERVER”； 服务选择“HTTP”； 目的地址转换为“HTTP_SERVER”

（5）定义访问规则，见表 7-2。

（6）定义路由，见表 7-3。

表 7-2　访问规则

允许内网用户访问 HTTP 服务器	源区域选择“内网”； 目的区域选择“SSN”，目的地址选择“HTTP_SERVER”；服务选择“HTTP”； 访问权限选择“允许”，并启用该规则
允许内网用户访问邮件服务器	源区域选择“内网”； 目的区域选择“SSN”，目的地址选择“MAIL_SERVER”；服务选择“POP3”，“SMTP”； 访问权限选择“允许”，并启用该规则
允许内网用户访问 FTP 服务器	源区域选择“内网”； 目的区域选择“SSN”，目的地址选择“FTP_SERVER”；服务选择“FTP”； 访问权限选择“允许”，并启用该规则
允许外网用户访问 HTTP 服务器	源区域选择“外网”； 目的区域选择“SSN”，目的地址选择“HTTP_SERVER”；服务选择“HTTP”； 访问权限选择“允许”，并启用该规则

表 7-3　路由

为内网用户访问 Internet 添加缺省路由	目的地址设为“0.0.0.0”； 网关地址设为“202.69.38.9”
添加回指路由，为发往内网的数据包指定路由	目的地址设为“192.168.0.0”； 网关地址设为“192.168.1.10”

实例 2：混合模式下通过 ADSL 拨号访问外网

混合模式下通过 ADSL 拨号访问外网，主要描述分公司网络卫士防火墙的配置，分公司的网络卫士防火墙工作在混合模式下，如图 7-8 所示。值得注意的是，分公司是通过 ADSL 拨号与外网进行连接的。

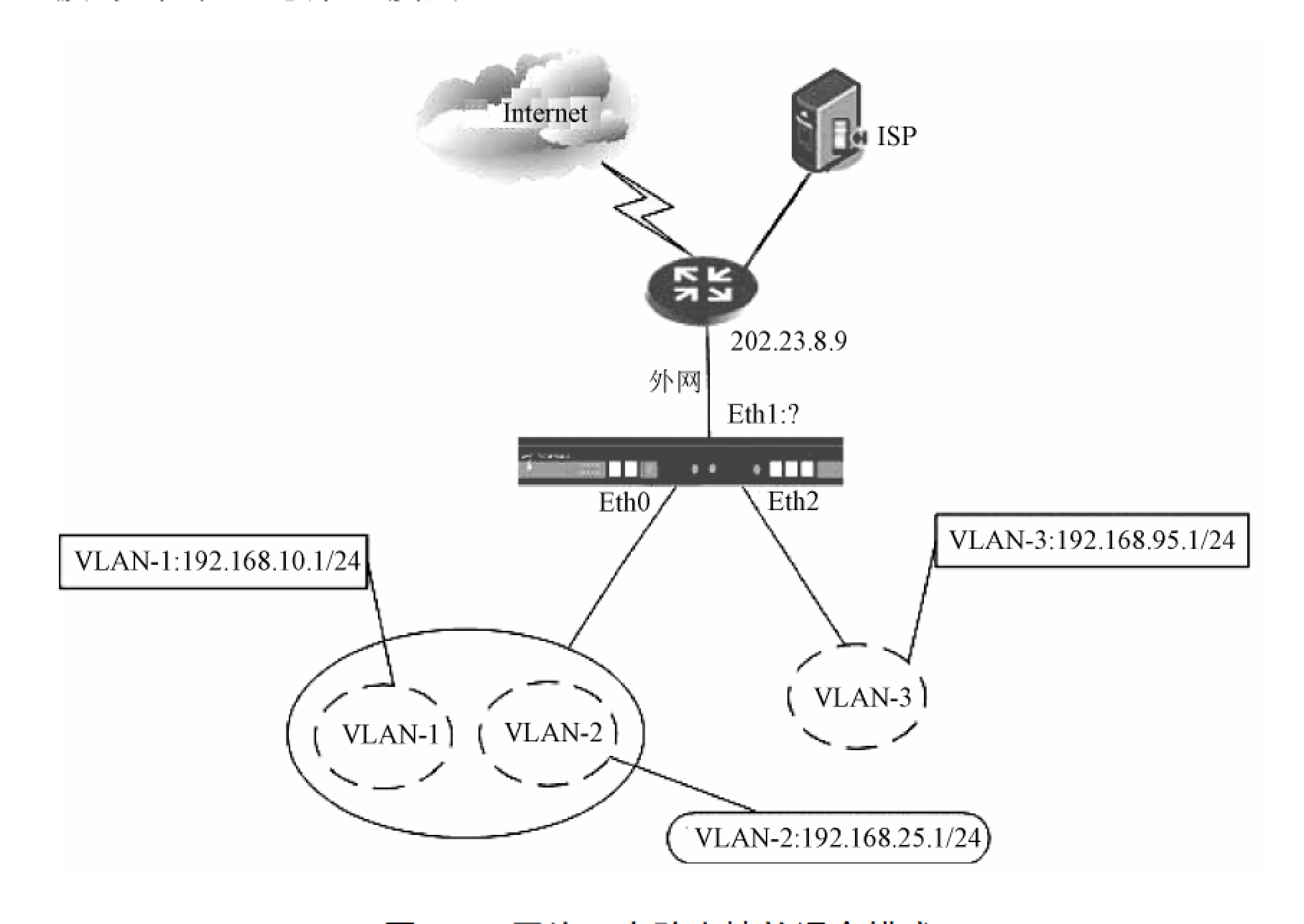


图 7-8　网络卫士防火墙的混合模式

1．网络状况

（1）分公司的网络卫士防火墙工作在混合模式下。Eth1 为路由接口，属于外网区域，通过路由器与外部网络及 ISP 相连（该接口由 ADSL 拨号获取公网 IP）；Eth0 和 Eth2 均为交换接口，Eth0 工作在 Trunk 方式下，Eth2 工作在 Access 方式下；Eth0 下连接着两个 VLAN，VLAN-1 和 VLAN-2；Eth3 下连接着 1 个 VLAN，VLAN-3。

（2）VLAN-1 的 IP 为 192.168.10.1/24；VLAN-2 的 IP 为 192.168.25.1/24；VLAN-3 的 IP 为 192.168.95.1/24。

（3）管理主机位于 VLAN-1 内。

2．用户需求

（1）防火墙通过 ADSL 拨号获取 eth1 的公网 IP 地址。

（2）VLAN-1 内的机器可以任意访问外网（NAT 方式），VLAN-2 和 VLAN-3 内的机器禁止访问外网，但允许 VLAN-2 访问 VLAN-3。

（3）外网的机器不能访问 VLAN-1 与 VLAN-2，但可以访问 VLAN-3。

3．配置步骤

（1）通过 CONSOLE 口登录网络卫士防火墙，配置基本信息。

进入 network 组件 topsec # network

添加 VLAN-1 topsec.network# vlan add id 1

配置 VLAN-1 的管理 IP topsec.network# interface vlan.0001 ip add 192.168.10.1 mask255.255.255.0

配置 eth0 接口为交换接口 topsec.network# interface eth0 switchport mode trunk

设置 eth0 接口属于 VLAN-1 topsec.network# interface eth0 switchport trunk allowed-vlan 0001

（2）管理员通过 VLAN-1 的管理 IP 登录网络卫士防火墙，并绑定 eth1 口和 ADSL 的拨号属性、设置区域资源及 VLAN。

设置区域（外网）绑定属性为“adsl”；权限设为允许访问。

添加 VLAN-2 管理 IP 设为“192.168.25.1”，MASK 设为“255.255.255.0”。

添加 VLAN-3 管理 IP 设为“192.168.95.1”，MASK 设为“255.255.255.0”。

设置 eth0 接口属于 VLAN-2，VLAN 范围设为“1-2”。

（3）设置接口。

设置接口 eth2 设置为“交换接口”；接口类型为“access”；VLAN 范围为“3”。

（4）设置 ADSL 拨号参数。

设置 ADSL 拨号参数接口设置为“eth1”；用户名和密码根据 ISP 服务商提供的参数值进行设置；绑定属性为“adsl”。

（5）定义访问规则，见表 7-4。

（6）定义地址转换规则。

VLAN-1 用户通过源地址转换访问外网：转换控制选择“源转换”；源 VLAN 选择“VLAN.0001”；目的区域选择“外网”；服务不选，表示全部服务；源地址转换为“adsl”。

表 7-4　实例 2 访问规则

禁止 VLAN-2 用户访问外网	源 VLAN 选择“VLAN.0002”；目的区域选择“外网”； 服务不选，表示全部服务；访问权限选择“拒绝”，并启用该规则
禁止 VLAN-3 用户访问外网	源 VLAN 选择“VLAN.0003”；目的区域选择“外网”； 服务不选，表示全部服务； 访问权限选择“拒绝”，并启用该规则
允许 VLAN-2 用户访问 VLAN-3	源 VLAN 选择“VLAN.0002”；目的 VLAN 选择“VLAN.0003”； 服务不选，表示全部服务； 访问权限选择“允许”，并启用该规则
禁止外网用户访问 VLAN-1	源区域选择“外网”；目的 VLAN 选择“VLAN.0001”； 服务不选，表示全部服务； 访问权限选择“拒绝”，并启用该规则
禁止外网用户访问 VLAN-2	源区域选择“外网”；目的 VLAN 选择“VLAN.0002”； 服务不选，表示全部服务； 访问权限选择“拒绝”，并启用该规则

（7）拨号。

在防火墙上通过选择网络管理→DSL 菜单，并单击“开始拨号”按钮进行 ADSL 拨号。建立 ADSL 连接成功后，在防火墙的路由表中会增加一条内网用户访问 Internet 的路由信息：

源为“0.0.0.0/0”；

目的为“0.0.0.0/0”；

网关地址为 ISP 分配的公网 IP 地址（如：169.254.125.124）；

接口为与 Eth1 口绑定的 ppp0 口（拨号成功后，系统自动创建了一个 ppp0 口）。

实例 3：建立 VPN 隧道

建立 VPN 隧道，主要介绍在如上所述的网络环境中，如何在总公司与分公司之间建立 IPSec VPN 隧道，其网络拓扑结构如图 7-9 所示。

1．网络状况

（1）总公司防火墙工作在路由模式下，接口 Eth1（IP：202.69.38.8）通过路由器与 Internet 相连；分公司防火墙工作在混合模式下，接口 Eth1 通过路由器与 Internet 相连，且 Eth1 口通过 ADSL 拨号获取公网 IP。

（2）总公司防火墙的 Eth0 口与 Eth2 口分别连接公司内网区和 SSN 区域，内网区有 3 个子网：192.168.2.0/24、192.168.3.0/24、192.168.1.0/24。

（3）分公司防火墙的 Eth0 口与 Eth2 口分别连接内网的 3 个 Vlan：VLAN-1、VLAN-2 和 VLAN-3，其中 VLAN-1 的 IP 为 192.168.10.1/24。

2．用户需求：

分公司的 VLAN-1 所在子网 192.168.10.0/24 与总公司子网 192.168.2.0/24 之间建立基于预共享密钥认证的 VPN 通信。

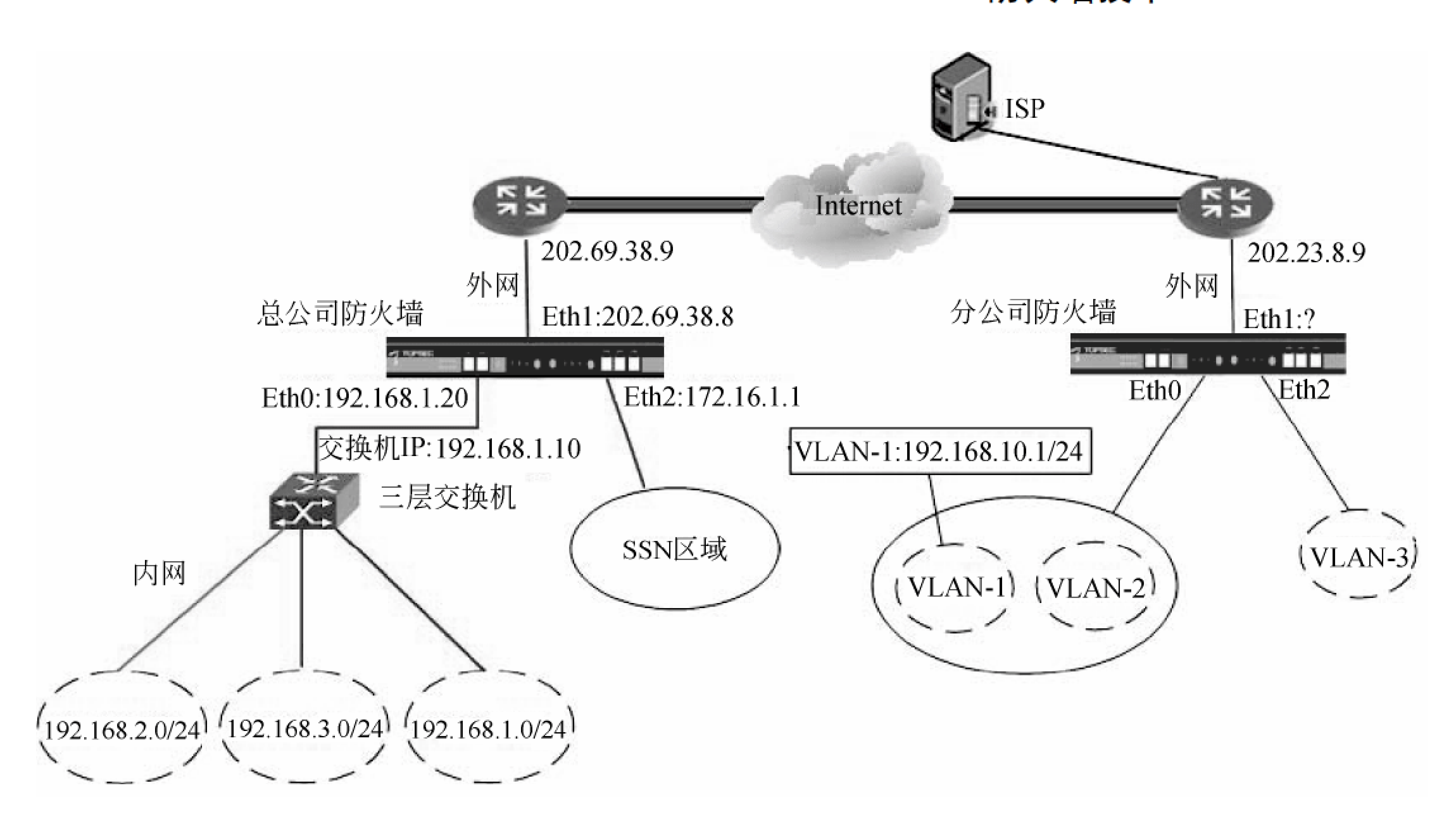


图 7-9 网络卫士防火墙的 VPN 隧道模式

3．配置步骤

（1）配置总公司防火墙，具体的配置步骤请参见案例 1。

（2）配置分公司防火墙，具体的配置步骤请参见案例 2。

下面只描述与建立 VPN 隧道有关的操作。

（3）在总公司防火墙上开放“IPSecVPN”服务。

开放 IPSecVPN 服务：服务名称为“IPSecVPN”；控制区域为“area_eth1”；控制地址为“any”。

（4）在分公司防火墙上开放服务。

开放 IPSecVPN 服务：服务名称为“IPSecVPN”；控制区域为“area_eth1”；控制地址为“any”。

（5）在总公司防火墙上绑定虚接口。

绑定虚接口：虚接口名为“ipsec0”；绑定接口名为“eth1”；接口地址为“202.69.38.8”。

（6）在分公司防火墙上绑定虚接口。

绑定虚接口：虚接口名为“ipsec0”；绑定接口名为“eth1”；接口地址为“0.0.0.0”。

（7）在总公司防火墙上添加静态隧道，隧道参数采用默认设置。

添加静态隧道：隧道名：zong-fen

IKE 协商模式：主模式

认证方式 = 预共享密钥，密钥 =123456

本地标识：@202_8

对方标识：@0_0

对方地址：0.0.0.0

本地子网：192.168.2.0

本地掩码：255.255.255.0

对方子网：192.168.10.0

对方掩码：255.255.255.0

主动发起协商：是

（8）在分公司防火墙上添加静态隧道，隧道参数采用默认设置。

添加静态隧道隧道名：fen-zong

IKE 协商模式：主模式

认证方式 = 预共享密钥，密钥 =123456

本地标识：@0_0

对方标识：@202_8

对方地址：202.69.38.8

本地子网：192.168.10.0

本地掩码：255.255.255.0

对方子网：192.168.2.0

对方掩码：255.255.255.0

主动发起协商：是

提 示

本案例中分公司防火墙采用的是 ADSL 拨号的方式，故其 IP 设置为 0.0.0.0。如果建立隧道的两台防火墙均为 ADSL 环境，则可以通过 DDNS 方式，利用域名来建立隧道。

实例 4：多种服务的防火墙配置

（1）局域网内共 5 个 VLAN，其中 VLAN1 用于网络设备管理，VLAN10、11、12 用于局域网内用户，VLAN20 为内部服务器，对应的子网规划：

VLAN1：192.168.0.0/24　GW：192.168.0.254

VLAN10：192.168.10.0/24　GW：192.168.10.254

VLAN11：192.168.11.0/24　GW：192.168.11.254

VLAN12：192.168.12.0/24　GW：192.168.12.254

VLAN20：192.168.20.0/24　GW：192.168.20.254

防火墙内口位于 VLAN1，分配 IP 为 192.168.0.253，OA Server 位于 VLAN20，分配 IP 为 192.168.20.250。

（2）SSN 内的服务器对 Internet 及内部局域网提供 Web、Email、FTP 服务，内部 OA 服务器对局域网用户及分支机构用户提供 OA 服务。

（3）从 ISP 那里申请到一段 61.144.102.0/29 段公网 IP，共 8 个 IP，缺省路由是 61.144.102.6，可用 IP 有 5 个，分配如下。

防火墙外口：61.144.102.1

Web：61.144.102.2

FTP：61.144.102.3

Email：61.144.102.4

备用：61.144.102.5

其中 SSN 那 3 台服务器的 IP 由防火墙实现一对一地址翻译。

（4）分支机构与防火墙建立 VPN 隧道访问内部 OA 服务器。

- 分支机构 1、2 也安装 VPN 网关直接与防火墙建立 Site-to-Site 的 VPN 隧道。
- ADSL 拨号分支机构与远程移动办公用户采用 VPN Client 软件与防火墙建立 Client-to-Server 的 VPN 隧道。

（5）访问控制需求如下。

- VLAN10 用户访问 Internet，24 小时允许 POP3、SMTP、DNS 服务，休息时间（周一至周五的下午 6 点至次日 9 点、周六周日全天）允许 HTTP。
- VLAN11 用户访问 Internet，24 小时允许 HTTP、POP3、SMTP、FTP、DNS。
- VLAN12 用户访问 Internet 及 SSN，24 小时所有服务不限制。
- 所有内部用户及 Internet 公网访问 SSN 内 WEB 的 HTTP、Email 的 POP3 和 SMTP、FTP 服务器的 FTP 服务 24 小时不限制。
- 分支机构通过 VPN 隧道访问内部 OA 服务器 24 小时不限。
- VLAN10、VLAN11 用户访问 Internet 作带宽限制最高 256Kbps，其中 VLAN11 优先级稍高。

其网络拓扑结构如图 7-10 所示。

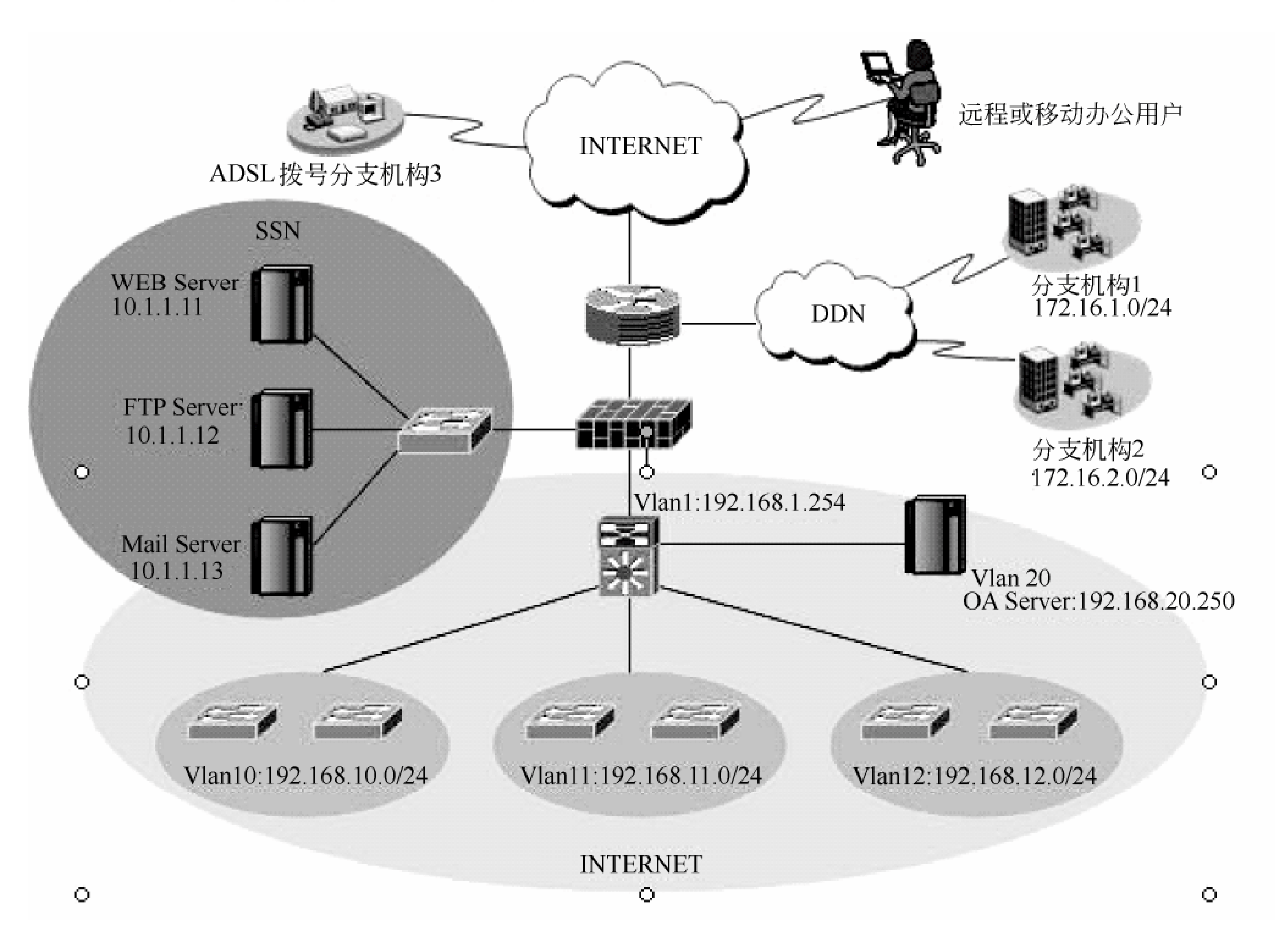


图 7-10　实例 4 网络拓扑结构

第 8 章　入侵检测

本章学习重点：

- 入侵检测基本原理
- 异常检测与误用检测
- 基于主机入侵检测系统与基于网络入侵检测系统
- Snort 系统安装与基本使用

8.1　入侵检测的概念与基本术语

系统安全一般由预防、侦查、响应 3 部分组成。安全管理者通常将大部分注意力放在预防和侦查上面，入侵检测是一种对威胁系统和网络安全的行为进行检测的技术，典型的入侵检测系统如图 8-1 所示。1980 年 James Anderson 在论文《计算机安全威胁监察与监控》中第一次提出入侵检测的概念，并推动了其发展。对入侵检测的概念与基本术语说明如下。

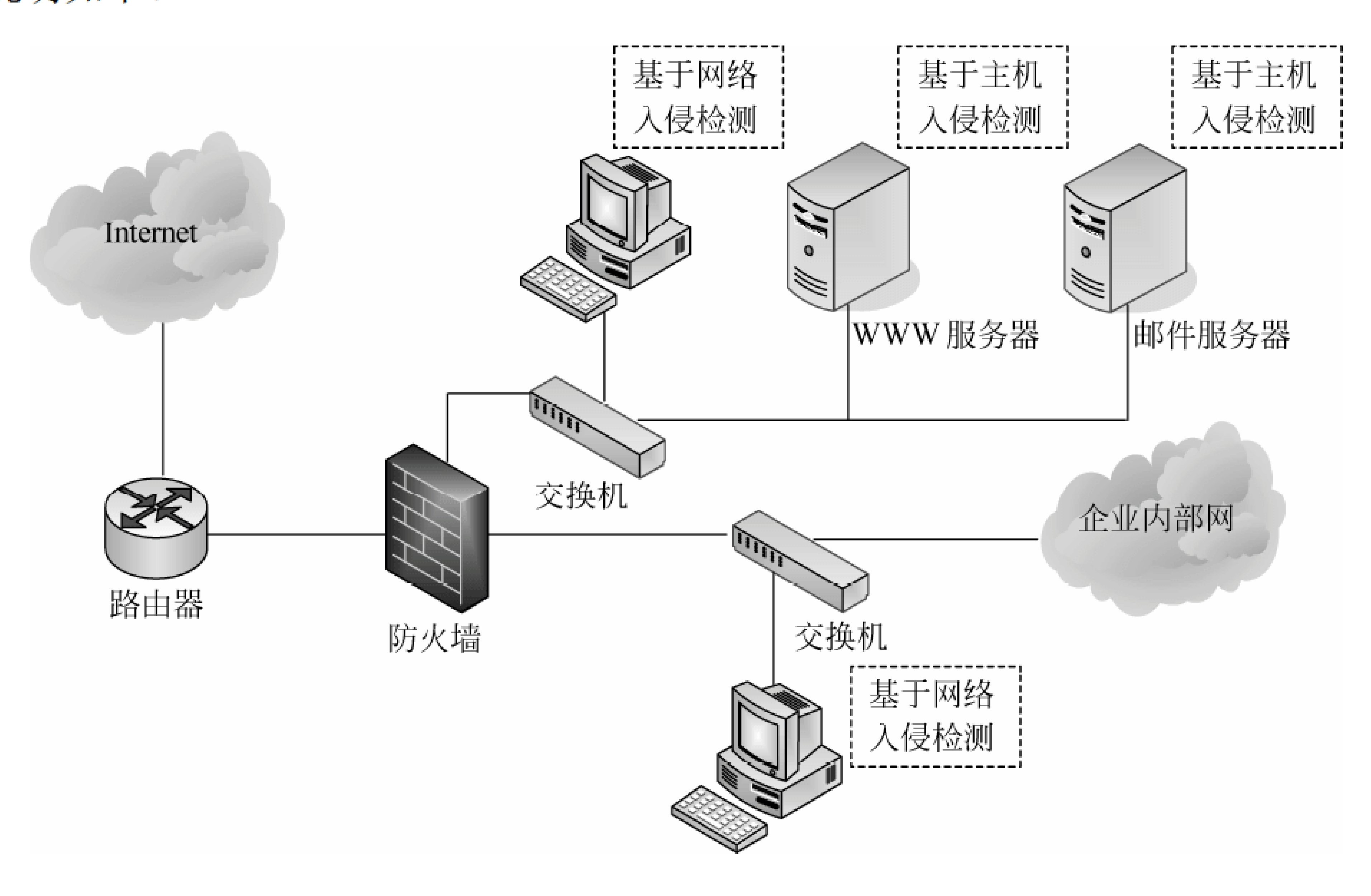


图 8-1　典型的入侵检测系统示意图

- **入侵**　指未经授权非法进入信息系统的行为，可能导致资源的滥用、不可信与不可用，该行为的实施者就是入侵者。
- **入侵过程**　一个入侵行为包含着大量的步骤，首先通过扫描收集目标系统的信息，然后判定目标系统存在的漏洞，通过系统漏洞获取系统访问权限，进入系统利用系统资源。

- **误报** 将正常的行为当作异常行为处理。
- **漏报** 将异常的行为当作正常行为处理。
- **入侵检测** 分析系统的行为并辨别是否是异常行为的过程。
- **入侵检测系统（IDS）** 持续检测系统行为，侦测系统异常行为的软硬件总和。
- **基于主机的入侵检测系统（HIDS）** 检测针对某一特定主机进行的入侵行为的软硬件总和。
- **基于网络的入侵检测系统（NIDS）** 检测针对某一网络或某一特定网段流量进行入侵行为的软硬件总和。
- **混杂模式** 在此模式下，网卡能够接收流经该网段的所有数据包流量而不用考虑数据包的目的地址。
- **入侵检测系统组成** 互联网工作小组将 IDS 分为事件产生器、事件分析器、响应单元和事件数据库 4 部分。事件产生器从计算环境中获得事件，并向系统的其他部分提供此事件；事件分析器用于分析数据；响应单元用于发出警报或采取主动响应措施；事件数据库用于存放各种数据。

图 8-2 给出了各部分之间的关系。

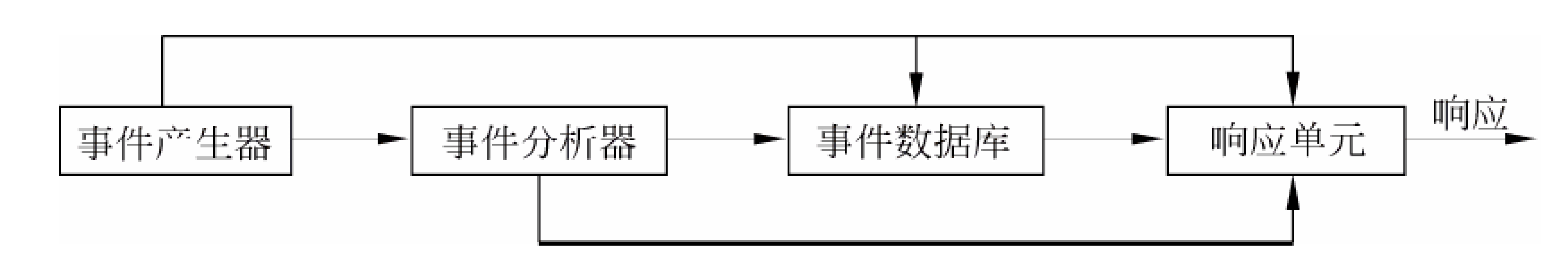


图 8-2 入侵检测系统组件

事件产生器接收到事件后，将事件转化成其他部件可以接受的格式发送给事件分析器，事件分析器接收到转化后的事件，分析该事件的意义（如异常，违反策略），然后将其发送给事件数据库进行备份以备查询，并发送给响应单元，响应单元接收到分析器的信息后会执行相应的响应。

8.2 入侵检测系统的检测机制

入侵检测系统的检测机制一般可以分为 3 种：基于异常的检测机制，基于特征的检测机制，以及两者混合的检测机制。

1. 异常检测

基于异常的检测，通过将系统或用户行为与正常行为进行比较来判别是否为入侵行为，通常会首先给出一个系统正常行为的特征列表，即“白名单”列表。然后将系统或用户行为特征和“白名单”中的行为特征进行比较，如果匹配，则判定系统或用户的行为是正常行为，否则，判定系统或用户的行为是入侵行为。特征一般由用户、用户组、应用程序、系统等的经验数据组成。然而给出的“白名单”列表往往不能代表所有可接受的行为，因此异常检测就需要不断学习，不断提取系统正常行为的特征进而更新“白名单”列表。

异常检测存在的主要问题有：非入侵行为的行为被分类成入侵行为，即误报问题；

未导致异常结果的入侵行为不能被检测出，即漏报问题；扫描的持续进行及列表的不断更新导致的计算量过大问题。

2．误用检测

不同于异常检测，误用检测假定每个入侵行为都能够用一个独特的模式或特征所代表，因此在系统中建立异常行为的特征库，然后将系统或用户的行为与特征库进行比较。若特征相互匹配，则判定系统或用户的行为是入侵行为，若不能匹配，则判定系统或用户行为是正常行为。在互联网中，存在着大量关于已知入侵检测行为特征的记录，这些特征能被入侵检测系统利用，特征库必须在工作同时进行更新。

误用检测存在的主要特征有：系统不能检测未知的、未被描述的攻击；系统不能预知新的攻击，只能检测出已发生过的攻击。

8.3 入侵检测系统

8.3.1 入侵检测系统的设计准则

系统设计必然要遵循一定的标准，入侵检测系统的设计准则包括以下几点。

（1）其配置结束后可以自我运行。

（2）工作时必须时刻保持积极的工作状态且自身不易被攻击。

（3）能够识别系统不常见的行为，每一个入侵检测系统都会遗漏一些异常行为，不过一个好的系统能够尽可能多地发现入侵行为。

（4）系统运行要尽可能减少对正常工作的影响。

（5）系统必须可控、可调试。

通过数据来源的不同，可以将入侵检测系统分为基于网络的入侵检测系统和基于主机的入侵检测系统。

8.3.2 基于网络的入侵检测系统（NIDS）

基于网络的入侵检测系统是将整个网络作为扫描范围，通过检测整个网络来发现网络上异常的，不恰当的或其他可能导致未授权、有害事件发生的事件。

NIDS 有几种不同的运行模式：一种是作为独立的机器，在混杂模式下检测所有的网络数据；另一种是将自己变为目标主机，检测流经自己的所有网络数据。

基于网络的入侵检测系统的各个组件之间通过共同工作进行预警，几个组件分别是：网络负载均衡器（Network Tap/Load Balancer）；网络传感器/监控器（Network Sensor / Monitoring）、分析器（Analyzer）、报警器（Alert Notifies）、命令级管理控制器（Command Console/Manager）、响应子系统（Response Subsystem）、数据库（Database）。图 8-2 给出了其具体的架构。

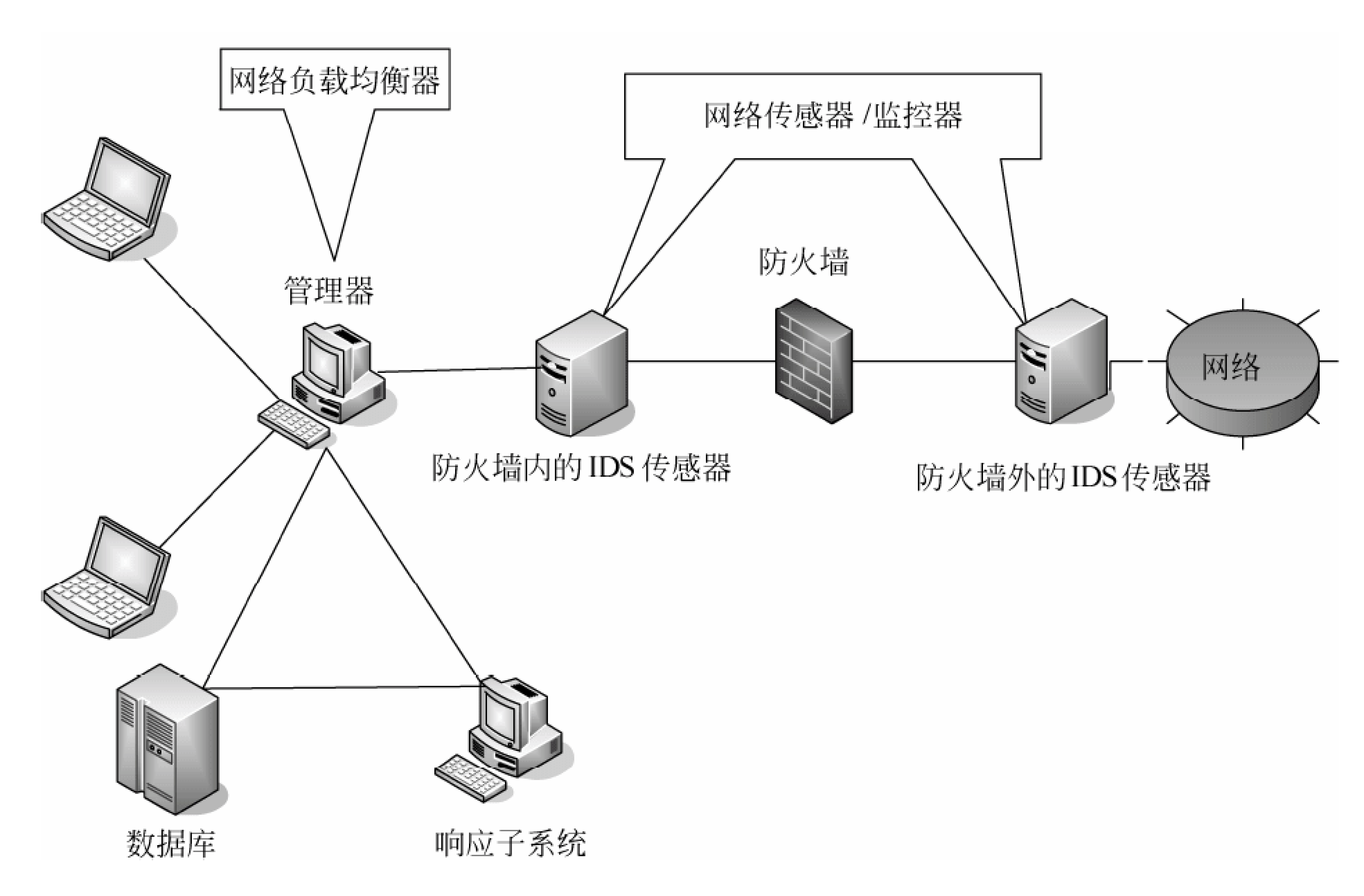


图 8-3　基于网络的入侵检测系统的部署

其中最关键的是传感器位置，直接影响着入侵系统接受网络数据的效率。传感器的部署取决于以下几种因素：被保护的内部网络的拓扑结构；组织所遵循的安全策略；实际工作中安全实践的类型。根据上述的几种因素，传感器的位置一般会选取在非军事区中，防火墙与网络之间，或网络关键点等位置。

8.3.3　基于主机的入侵检测系统（HIDS）

系统的信息误用问题不只是外部的入侵造成的，更多的是来自于系统内部。为避免系统内部的攻击，安全专家将检测转向组织网络的内部，检测针对本地主机入侵行为的系统被称为基于主机的入侵检测系统（HIDS）。

基于主机的入侵检测是在单一主机上进行恶意行为检测的技术。HIDS 部署在单一的目标主机上，利用软件检测主机的具体日志信息，如 Windows 系统中的系统日志、事件日志、安全日志或 UNIX 系统中的系统日志。当这些文件发生了变化，HIDS 就将相关事件与攻击特征表进行匹配，如果匹配，那判定系统内有攻击发生。

HIDS 可以部署在单一主机上，同样也可以部署在远程主机上，或部署在网段上来检测整个网段。HIDS 的缺点在于大量需要检测的原始数据造成分析程序处理能力的增加以及检阅数据的安全工作人员数量的增加。

8.3.4　NIDS 与 HIDS 比较

NIDS 与 HIDS 在网络中部署位置不同，因此在实际应用中各有优缺点。

与 HIDS 相比，NIDS 的优点主要表现以下几个方面。

（1）可以检测到 HIDS 不能检测到的攻击：NIDS 在传输层监测网络流量，不仅查看

数据包的地址，同样查看数据包的端口地址，而 HIDS 是不具备这种的能力的，因此 NIDS 能够检测到某些 HIDS 漏掉的攻击。

（2）实时监测：NIDS 处于关键的网络节点中，可以实时检测网络的外部攻击。

（3）可以检测到未成功的入侵行为：HIDS 处于被保护的内部网络中，而大部分攻击都会被挡在防火墙之外，偶尔有越过第一道防火墙的攻击，也会被内部防火墙和非军事区中的服务所拒绝，因此 HIDS 很难捕捉到这些攻击。而 NIDS 则可以捕捉到这些攻击，并记录这些攻击的频率。

尽管 NIDS 可以很好地检测所有流入网络的通信，但也存在着一定的问题。

（1）和 HIDS 比，NIDS 拥有盲区，为部署在组织网络的边缘地带，NIDS 对整个内部网络是不了解的，从而产生盲区。

（2）尽管可以对包头等一些未加密的部分进行检测，但对数据包其他加密的部分，NIDS 是不能解密的。而 HIDS 可以不用考虑这些问题。

8.3.5 其他类型的入侵检测系统

在入侵检测领域除了 NIDS、HIDS 系统被广泛使用，还有一些服务目标更加具体的入侵检测工具，共同发挥着入侵检测的作用。

1. 系统完整性验证者（SIVs）

系统完整性验证者一直监测系统中的核心文件（例如系统文件或注册表）来检测是否被入侵者更改。另外 SIVs 也可以检测其他系统部件的数据，如可以检测到具有普通权限的用户越权访问系统的行为。

2. 日志文件监督（LFM）

LFM 监测网络服务创建的日志记录，寻找日志文件中的 system trends、tendencies、pattern 等内容，并将其与关键字进行匹配来判断入侵者是否正在攻击。

3. 蜜罐

蜜罐也可认为是一个“陷阱”，诱使入侵者对其进行攻击从而获取攻击者攻击工具和攻击方法的信息。蜜罐是一个附件工具，在保护系统安全的很多方面发挥着巨大的作用。

蜜罐系统是一个包含漏洞的系统，给入侵者提供一个容易入侵攻击的机会。由于蜜罐不会提供其他任何服务，因此所有对其进行连接的尝试都被视为是可疑的。蜜罐的另一个用途是拖延攻击者对真正目标的攻击，让攻击者在蜜罐上浪费时间，从而使最初的攻击目标受到了保护，真正有价值的内容不受侵犯。

8.4 入侵检测系统实现

入侵检测系统对收集的数据进行分析并以此判断是否为入侵行为，具体的实现方法有以下几种：特征检测、统计检测和专家系统。

1. 特征检测

对已知的攻击或入侵方式做确定性的描述，形成相应的事件模式，当被审计的事件与已知的入侵事件模式相匹配时，即报警。原理上与专家系统相仿。其检测方法上与计算机病毒的检测方式类似。目前基于特征描述的模式匹配应用较为广泛，特征检测的准确率较高，但对无经验知识的入侵与攻击行为是无效的。

2. 统计检测

统计模型常用异常检测，在统计模型中常用的测量参数包括审计事件的数量、间隔时间、资源消耗情况等。常用的入侵检测有 5 种统计模型，见表 8-1。

表 8-1　常用的入侵检测统计模型

统计模型	描述
操作模型	该模型假设异常可通过测量结果与一些固定指标相比较得到，固定指标可以根据经验值或一段时间内的统计平均得到，举例来说，在短时间内多次失败的登录很有可能是口令尝试攻击
方差	计算参数的方差，设定其置信区间，当测量值超过置信区间的范围时表明有可能是异常
多元模型	操作模型的扩展，通过同时分析多个参数实现检测
马尔柯夫过程模型	将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化，当一个事件发生时，如果在状态转移矩阵中该事件的转移概率较小，那么就可能当作是异常事件
时间序列分析	将事件计数与资源耗用根据时间排成序列，如果一个新事件在该时间发生的概率较低，则该事件可能是入侵

统计方法的最大优点是可以“学习”用户的使用习惯，从而具有较高检出率与可用性。但是它的“学习”能力也给入侵者以机会通过逐步“训练”使入侵事件符合正常操作的统计规律，从而欺骗入侵检测系统。

3. 专家系统

用专家系统对入侵进行检测针对的大多数是有特征的入侵行为。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达，是入侵检测专家系统的关键。在系统实现中，将有关入侵的知识转化为 if-then 结构（也可以是复合结构），if 部分为入侵特征，then 部分是系统防范措施，运用专家系统防范入侵行为的有效性完全取决于专家系统知识库的完备性。

8.5 入侵检测系统产品的选择

入侵检测系统产品的选择要多方面地考虑，具体因素如下。

- **价格**　系统价格以及特征库升级与维护的费用，性能价格比以及要保护系统的价值都是选择入侵检测系统时的重要因素。

- **网络的部署环境**　如果在 512KB 或 2MB 专线上部署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，入侵检测系统的最大可处理流量是一个非常重要的指标。
- **入侵检测系统对于异常行为的敏感度**　有些常用的躲开入侵检测的方法，如分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等，是入侵检测系统必须考虑的要素。
- **产品的可扩展性**　系统的选用应该具有良好的扩展性以满足网络日益扩大及日后升级的需要。
- **软硬件情况**　产品支持的入侵特征数，产品有哪些响应方法，系统支持的传感器数目、最大数据库大小等都是选择入侵检测系统产品时需要考虑的因素。
- **误报率与漏报率**　判定一个入侵检测系统的好坏，一般是通过误报率与漏报率两个指标进行分析。误报率即将一个正常的行为当作入侵行为而发出警报的概率，漏报率则是把一个异常的行为当作正常行为而没有发出警报的概率。

8.6 入侵检测的发展趋势

随着网络技术的发展，人们不断地研究着新的入侵检测技术，入侵检测技术的发展方向大致有以下几个。

- **大规模分布式入侵检测**　传统的入侵检测技术一般只局限于单一的主机或网络框架，不能适应大规模网络的监测，不同的入侵检测系统之间也不能协同工作。因此，必须发展大规模的分布式入侵检测技术。所谓分布式入侵检测有两层含义：第一层含义，即针对分布式网络攻击的检测方法；第二层含义即使用分布式的方法来检测分布式的攻击，其中的关键技术为检测信息的协同处理与入侵攻击的全局信息的提取。
- **智能化入侵检测**　即用智能化的方法与手段来进行入侵检测。所谓的智能化方法，现阶段常用的有神经网络、遗传算法、模糊技术、免疫原理等方法，这些方法常用于入侵特征的辨识与泛化。应用智能体的概念来进行入侵检测也有所尝试。
- **入侵检测的数据融合技术**　目前的 IDS 还存在着很多缺陷：首先，目前的技术还不能对付训练有素的黑客的复杂的攻击；其次，系统的误报率太高；最后，系统对大量的数据处理，非但无助于解决问题，还降低了处理能力。数据融合技术是解决这一系列问题的好方法。
- **全面的安全防御方案**　即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测多方位全面对所关注的网络做全面的评估，并且结合防火墙，病毒防护以及电子商务技术，提供完整的网络安全保障。

8.7 Snort 简介

Snort 是一种广泛使用的开源入侵检测系统，作为一个能够明确阐述入侵检测基本理

论的入侵检测系统，Snort 有以下几种特性。

（1）它是一个免费的程序，在 www.snort.org 上可以免费下载程序并取得产品文档。最初它是为 UNIX 设计的，但现在同样可以为 Windows 系统服务。

（2）Snort 容易操作，尽管它被创作者认为是“轻量级”的入侵检测系统，但也有足够的能力应付“麻烦的”系统。

8.7.1 Snort 的工作原理

从本质上来说，Snort 是一个可高度设置的包嗅探器。包嗅探器就是对流经的数据包进行窃听或嗅探的程序。同时，Snort 也具有 IDS 的功能，可以分析系统日志来检测入侵行为，并且可以实时检查网络数据。

当嗅探到来自网络的数据包之后，Snort 预处理器会先查看数据包的头部，然后决定是否检测里面的内容，Snort 规则的第一部分明确规定了哪种类型的数据包可以保留。

8.7.2 Snort 在 Windows 下的安装与部署

安装平台：Windows Server 2003，MySQL，Apache，PHP5。

需要的软件包如下。

- **Snort_2_6_1_1_Installer.exe**　Windows 版本的 Snort 安装包。
- **Snortrules-snapshot-CURRENT.tar.gz**　snort 规则库。
- **WinPcap 4.1.2**　网络数据包截取驱动程序。

以上软件均可以在网上直接下载获取。

1．安装 WinPcap

按向导提示完成即可（有时会提示重启计算机）使网卡处于混杂模式，能够抓取数据包。安装界面如图 8-4 所示。

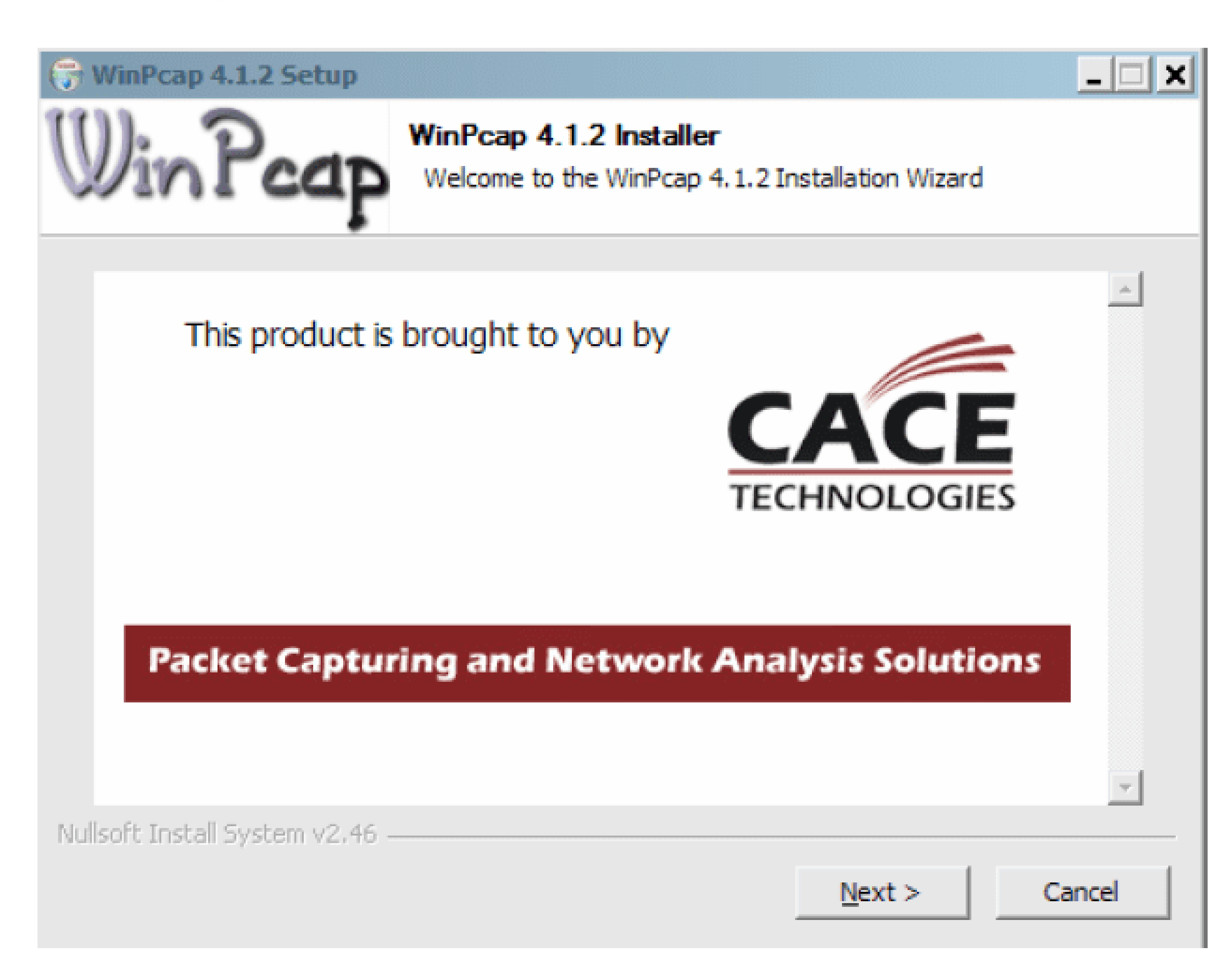


图 8-4　WinPcap 的安装

2. 安装 Snort

采用默认安装完成即可。

安装完成后使用下列命令行验证是否成功。

```
C:\Snort\bin>snort.exe -W
```

出现与图 8-5 类似的画面即表示安装成功。

```
C:\>snort\bin\snort.exe -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.8.6.1-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 39)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
           Copyright (C) 1998-2010 Sourcefire, Inc., et al.
           Using PCRE version: 7.4 2007-09-21
           Using ZLIB version: 1.2.3

Interface  Device                                      Description
-------------------------------------------------------------------------------
        1  \Device\NPF_{6FCD3D92-C3CF-478E-86BE-3BCFBC10D9AD}  Marvell Gigabit Ethernet Controller (Microsoft's Packet Scheduler)

        2  \Device\NPF_{B71929D6-5FC4-4C05-AA3E-2EC84E0D8A37}  MS Tunnel Interface Driver

C:\>_
```

图 8-5　Sonrt 的启动画面

8.7.3　启动 Snort

Snort 运行中分为 3 个模式：嗅探器模式、日志记录模式、IDS 模式。

1. 嗅探器模式

以嗅探器模式启动 Snort 是最简单的一种方式。在这个模式中，Snort 对所有的数据包进行嗅探。在这种模式下启动 Snort 使用命令：

```
$ snort -dev
```

-d 选项说明 Snort 要检测所有网络层的数据包头（TCP、UDP、ICMP）。

-e 选项说明 Snort 检测数据链路层的头。

-v 就是在包嗅探器模式下启动。

图 8-6 为 Snort 启动后某一界面的截图。

2. 日志记录模式

Snort 也可以记录数据的行为，这一个模式称为包日志记录模式。-l 选项说明 Snort 指定一个目录用于存储日志，使用这个语法可以存储数据包的日志。

```
$ snort -dev -l <log directory>
```

这个命令可以在包日志记录模式下记录数据包的日志，所有的输出都以 ASCII 的文本形式出现。如果需要二进制输出，Snort 可以生成一个 TCPDump 来格式化文件，在很多 IDS 中，TCPDump 格式化是很普遍的。在记录日志方面，二进制数据比 ASCII 快，因为 IDS 不用把数据包里面的内容翻译成文本数据。Snort 使用-b 选项说明由二进制来

记录日志，并使用-L 选项来规定二进制日志文件存放的位置，例如：

```
$ snort -dev -b -L {log file}
```

```
Packet Wire Totals:
   Received:            24
   Analyzed:            23 (95.833%)
    Dropped:             0 (0.000%)
Outstanding:             1 (4.167%)
===============================================================================
Breakdown by protocol (includes rebuilt packets):
      ETH: 23           (100.000%)
  ETHdisc: 0            (0.000%)
     VLAN: 0            (0.000%)
     IPV6: 0            (0.000%)
  IP6 EXT: 0            (0.000%)
  IP6opts: 0            (0.000%)
  IP6disc: 0            (0.000%)
      IP4: 20           (86.957%)
  IP4disc: 0            (0.000%)
    TCP 6: 0            (0.000%)
    UDP 6: 0            (0.000%)
    ICMP6: 0            (0.000%)
  ICMP-IP: 0            (0.000%)
      TCP: 0            (0.000%)
      UDP: 20           (86.957%)
     ICMP: 0            (0.000%)
  TCPdisc: 0            (0.000%)
  UDPdisc: 0            (0.000%)
  ICMPdis: 0            (0.000%)
     FRAG: 0            (0.000%)
   FRAG 6: 0            (0.000%)
      ARP: 0            (0.000%)
    EAPOL: 0            (0.000%)
  ETHLOOP: 0            (0.000%)
```

图 8-6 Snort 的输出截图

3. IDS 模式

在 IDS 模式和包日志记录模式中，唯一不同的就是规则的设置。在包日志记录中，Snort 抓取并记录其所监测到的所有数据包。当增加规则后，Snort 会对其所记录的东西根据规则进行过滤。规则一般都存放在预先制定的文件中，被组织成标准的文本格式。

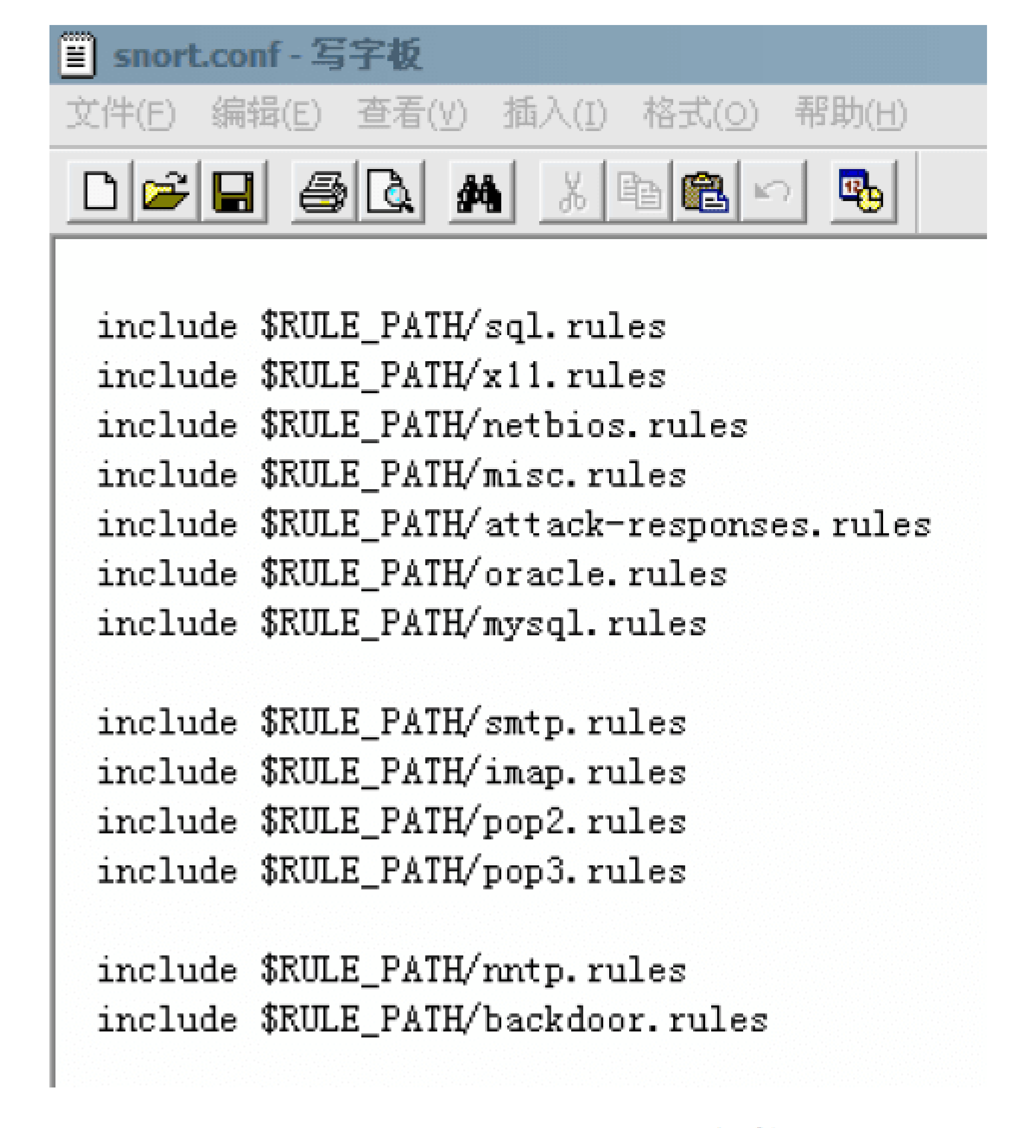


图 8-7 snort.conf 的内容截图

因为会有很多不同类型的规则，很自然地就要创建多个具体的规则文件并将其汇总在一个配置文件中，默认的配置文件是 snort.conf，配置文件用于多种目的，例如指定哪些网络可以被认为是安全的，哪些网络有潜在的威胁。snort.conf 提供的一个服务是引用每一个行为规则文件。在 Snort 会话中通过读取文件引用这些文件。读取文件就是打开规则文件并将这些规则读入行为规则数据库中。

图 8-7 给出了 snort.conf 文件的部分列表截图。

在 IDS 模式下启动 Snort，使用的命令与包日志记录模式类似并要加一个配置文件，配置文件提供了 Snort 规则的入口，例如：

```
$ snort -dev -l /snort/logs -c /snort/etc/snort.conf
```

在这个模式中，Snort 检查每一个规则中规定需要检查的包数据，如果其中有可疑数据，就会采取具体措施。

习　　题

一、选择题

1. 对于一个入侵，下列最合适的描述是（　　）。
   A. 与安全事故类似
   B. 各种试图超越权限设置的恶意使用
   C. 任何侵犯或试图侵犯你的安全策略的行为
   D. 任何使用或试图使用系统资源用于犯罪目的的行为
2. 下列哪种安全策略可用于最小特权原则的理念？（　　）
   A. 白名单　　B. 严格禁止
   C. 宽松的控制　　D. 黑名单
3. 如果一个 IDS 上报了一个异常行为，但该行为是正常的，那么 IDS 犯了什么错误？（　　）
   A. 误报　　B. 漏报
   C. 混合式错误　　D. 版本出错
4. 哪种入侵者是最危险的，为什么？（　　）
   A. 外部入侵者，因为他们在攻击之前会大量地收集目标系统的信息
   B. 内部入侵者，因为他们掌握更多关于系统的信息
   C. 外部入侵者，因为大部分入侵者都在外部
   D. 内部入侵者，因为很多外部入侵者都是新手
5. 对于有特征的入侵行为，哪种类型的入侵检测更适用？（　　）
   A. 误用检测　　B. 异常检测
   C. 恶意检测　　D. 外部检测
6. IDS 规则的目的是什么？（　　）
   A. 告诉 IDS 检测哪些端口
   B. 限制系统行为，如果违反了，就触发警报
   C. 告诉 IDS 哪些包需要被监测，并在包中检测什么内容
   D. 告诉防火墙哪些数据包可以穿过 IDS
7. 什么软件可以阅读其所在网络的数据？（　　）
   A. 特征数据库
   B. 包嗅探器
   C. 数据包分析引擎
   D. 网络扫描
8. 哪种 IDS 可以检测特定网段的所有流量？（　　）
   A. 基于网络的 IDS
   B. 基于特征的 IDS
   C. 基于主机的 IDS
   D. 基于知识的 IDS
9. 哪种类型的 IDS 可以用来标识外来攻击的？（　　）
   A. 在 DMZ 区的 HIDS
   B. 在防火墙与内部网络之间的 NIDS
   C. 在外部网络与防火墙之间的 NIDS
   D. 在 DMZ 区的 NIDS
10. 当选择 IDS 时，哪些因素是你要考虑的（多选）？（　　）
   A. 价格
   B. 配置与维护 IDS 所需要的知识与人力
   C. 互联网类型
   D. 你所在的组织的安全策略

二、问答题

1. 入侵检测系统都有哪些检测机制，其原理是什么？
2. 入侵检测系统是如何分类的，其设计准则是什么？

课后实践

1．阅读一篇与网络安全相关的报告，在安全领域，技术是不断地更新的，安全人员

的知识也在不停地更新，所以建议阅读一篇安全专家的最新的安全技术报告，访问 SANS 站点（www.sans.org/rr），在“categories”上选择 Intrusion Detection，选择站点内的任意一篇文档，简要写出该文档的要点和你所感兴趣的知识点。

2. 对于入侵检测系统，只有在操作以后才会对其原理有更深的理解。在前面已经简单地介绍了 Snort 的系统，为了更好地了解它的特性与操作流程，建议尝试使用 Snort：访问 Snort（www.snort.org），访问站点内的文档页面，然后使用 Snort Users Manual、SNORT FAQ、Snort Setup Guide。

结束后回答下列问题：

（1）列举出 snort 的 3 个模式。

（2）解释规则中规则头部与规则选项的区别。

（3）Snort 是 NIDS 还是 HIDS，为什么？

3. 假如你是一个小型网络服务提供商的安全管理员，你的上司让你负责为用户部署 IDS，现在你有两种选择：一种方案是选择基于主机的入侵检测系统，运行在用户的客户端上，鉴于大部分客户都使用 Windows 系统，因此只需要负责 Windows 操作系统即可，但是这样你必须说服客户将其安装到他们的电脑上，从而保护他们的主机；还有一种方案是选择基于网络的入侵检测系统，部署在用户使用的网络上，这个入侵检测系统可适用于 Windows 和 UINX 系统，花费较低，部署起来相对简单。

当你遇到该情况，首先对于这两类产品，分别列举出不少于 3 种具体产品出来，然后决定在这几个产品中选择哪种产品，最后解释一下为何要选择该产品而放弃其他产品。

第 9 章　系统安全扫描技术

本章学习重点：

- 理解系统安全扫描的含义
- 对操作系统和 TCP/IP 栈进行指纹识别
- 识别系统的安全漏洞
- 学习使用扫描工具
- 对系统评估做出详细的计划

9.1　系统安全扫描的技术基础

安全扫描是对系统评估以发现所有已知漏洞的过程。通常情况下，攻击者会首先对系统进行扫描，发现漏洞后再实施攻击。因此，用户也应该及时对系统进行扫描，发现并修补所存在的漏洞，消除安全隐患。扫描的过程非常简单，分为以下几个步骤。

（1）为操作系统创建一个列表，列表中包含了目前所有已知的安全漏洞（有很多可用的资源可以帮助用户完成这个步骤）。

（2）对列表中的每一个漏洞进行检查以确定其是否存在于系统中（也有很多现成的工具可以帮助完成这一步骤）。

（3）记录系统存在的漏洞。

（4）根据严重程度以及处理时所花费的成本对存在的漏洞划分等级。

（5）根据情况采取修补措施。

事实上，当用户开始真正扫描系统的时候，这些步骤要复杂的多。下面章节中，将会给出帮助用户创建漏洞列表以及选择安全扫描工具的一系列资源。

1．创建漏洞列表

系统安全扫描过程的第一步是创建一个包含当前所有安全漏洞的列表。在互联网上存在很多优秀的资源可以用来帮助完成这个步骤。附表 A-1 列出了维护着最新漏洞列表的网站，这对用户的帮助非常大，用户可以参考。

2．选择安全扫描工具

建立完成安全漏洞列表之后，用户要对列表上的每一个漏洞进行检测。在网络上有很多用户可用的资源来完成这一步骤。用户可以雇佣提供评估服务的公司，或使用多种自动工具来完成这项繁琐的工作。

雇佣第三方来执行评估的优点是用户不需要自己处理这些事情。大部分工作就是对扫描工具进行正确设置以及创建公司处理的漏洞报告。事实上，法律诉讼、产业标准或是投资要求等多种情况，都需要第三方进行外部评估。雇佣外部公司的缺点是用户很难

控制评估的完成过程。用户同样失去了及时评估系统的能力。另外，这样的成本会很高，并且很可能不是很灵活。

不论用户是自己完成评估还是雇佣他人来完成评估，方法基本是一样的。用户的目标是发现所有能够被发现的漏洞，然后减少或消除这些漏洞。需要注意的是，并不是每一个漏洞都值得处理。在考虑需要处理哪一个漏洞的时候，要考虑到漏洞被利用的可能性以及处理的开销。为了讨论方便，假设用户自己扫描系统的安全漏洞。用户可以从多个工具箱中选择工具。附表 A-2 列出了用户可以获得安全扫描软件的网站（当然，这只包含了一部分列表，还有很多其他的扫描工具是可用的）。在本章剩下的部分，将会使用 Nessus 扫描工具进行讨论。

用户需要花费一些时间找到支持自己操作系统的产品，并且了解每一种产品的功能特性。从供应商的文件入手，寻找关于产品使用的所有网页资源以及使用建议。用户也可以翻阅书籍。出版商已经注意到了安全话题在 IP 领域的发展趋势，所以关于安全话题的图书数量不断地增长。无论用户如何收集信息，都要了解所选择的扫描工具，然后准备开始扫描。

9.2 操作系统指纹识别工具

对系统进行扫描的第一个任务是找出计算机上运行的操作系统。检查远程计算机上运行的操作系统的过程叫做操作系统指纹识别。大多数的攻击者只针对一种操作系统，甚至只针对特定版本的操作系统进行攻击。识别计算机运行的操作系统之后，用户就可以检查系统安全漏洞了。漏洞检查过程就是参照特定操作系统已知漏洞的指纹信息进行对比。大多数安全扫描工具，都参考已知的漏洞数据库来创建进一步的行动列表。保持漏洞数据库的及时更新是非常重要的。就像病毒签名数据库，全面评估的有效性相当程度上依赖于数据库的状态。

根据用户的需要，可以进行不同复杂程度的操作系统指纹识别会话扫描。大多数扫描工具能够提供较为复杂详细的操作系统指纹信息。如果用户只需要操作系统的指纹信息，有多种工具可供选择。附表 A-3 列出了可以使用来识别操作系统的 3 种常见工具。

不同工具使用不同的技术来识别操作系统类型，但所有工具的原理都是一致的，都是利用通信如何建立、如何维护的知识对操作系统进行识别。不同的操作系统处理网络通信是不同的，在同一种操作系统的不同版本之间甚至也存在明显的差异。操作系统的指纹识别功能通常发送针对目标计算机而设计的数据包，并通过检验计算机的响应来确定操作系统。

9.3 网络和服务器扫描工具

确定目标计算机运行的操作系统之后，需要确定计算机上运行的软件。用户可以通过询问开放的端口号（很可能在操作系统识别的过程中就已经获得了系统的开放端口信息）并分析计算机的响应来完成这个步骤。在这个步骤中，需要用到另外一个数据库。用户可以尝试下面这个方法：使用远程登录来连接系统上所有开放的端口号。使用下面

这个命令来连接一个本地计算机（127.0.0.1，通常叫做本地主机）上的 80 端口：

```
$ telnet 127.0.0.1 80
```

按几次 Enter 键，就会收到计算机的响应。图 9-1 给出了在一个运行着 Windows XP 系统的计算机上输入 telnet 之后的响应。

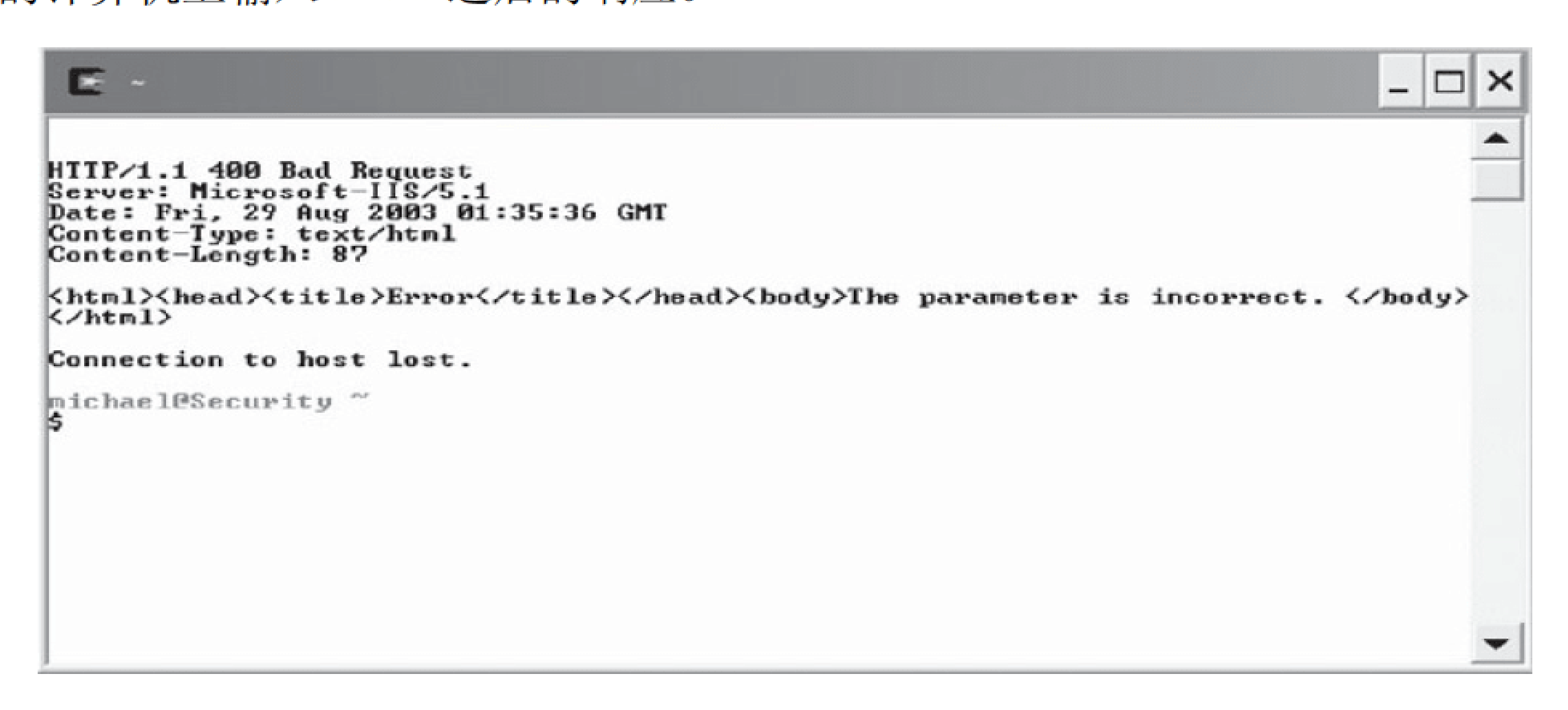


图 9-1　运行 telnet 命令后的响应

即使用户只是询问，但有些应用程序也会给出很多信息。例如用户连接一个端口，然后发送一个或两个回车，监视端口的程序就会为未知的程序产生欢迎信息。这种欢迎信息叫做标语。对于系统之间的对话，标语起到了很好的作用，但当用户想要加固系统的时候标语信息就会暴露更多的系统信息。因此，用户应该找到抑制或改变标语信息的方法来避免向攻击者透漏信息。例如，通过下面这个命令来连接本地计算机上的 21 号端口（21 号端口是大多数 FTP 服务器监听的端口）：

```
$ telnet 127.0.0.1 21
```

连接建立之后就会接收到一个标语信息。图 9-2 给出了运行 Windows XP 的计算机在收到 telnet 命令之后的反应。

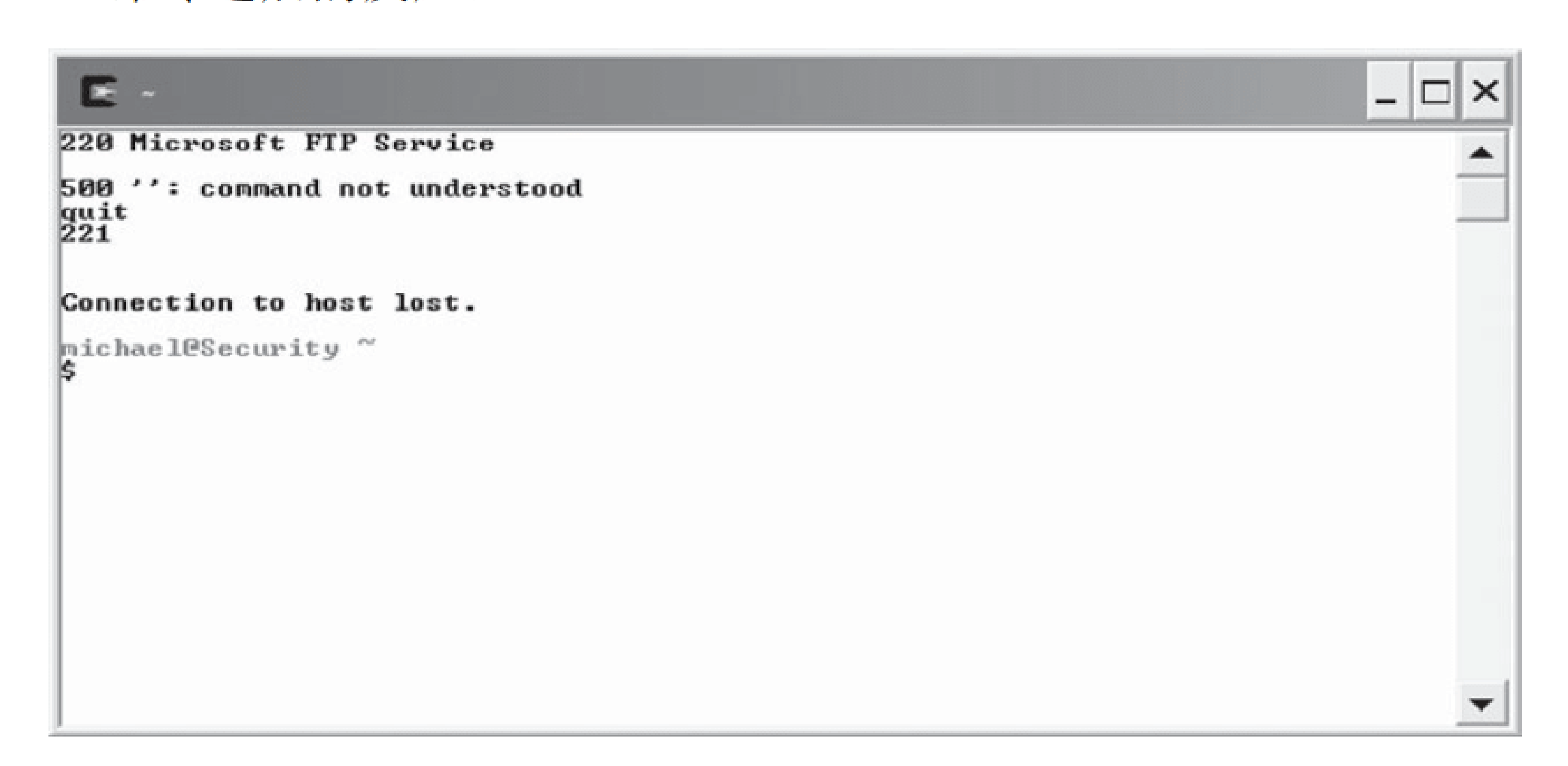


图 9-2　运行 telnet 命令之后的响应

扫描程序利用系统提供的标语信息来检测运行在计算机上的程序及其版本。同时这

些信息可以被用来寻找漏洞数据库中相关的软件漏洞。

9.4 IP栈指纹识别

Internet 协议（IP）栈指纹识别是用来进行操作系统指纹识别最重要的工具。不同的操作系统，甚至是同一种操作系统的不同版本都以不同的方式处理通信。向目标计算机发送专门构造的网络数据包，然后分析收到的响应，就能够判断出目标计算机上的操作系统。

下面介绍几种对操作系统进行指纹识别的工具。

（1）Nmap 扫描工具有 9 种独立的测试。在每种测试中，Nmap 同时向目标计算机的 3 种端口发送一定数量的 TCP 和 UDP 数据包。这 3 种端口是开放的 TCP 端口、关闭的 TCP 端口和关闭的 UDP 端口。每个数据包都设置了详细的标志位来引起特定的响应。收到响应数据包后，对数据包进行分析，并和已知 IP 栈的响应进行比较。如果结果匹配，就说明在目标计算机上运行着相应的 IP 栈和操作系统。使用这种指纹识别方法，Nmap 能够识别超过 870 种操作系统指纹。

（2）Sprint 扫描工具是另一种创建 IP 和操作系统指纹的工具，能以主动方式或被动方式运行。在主动方式中，Sprint 主动和目标计算机建立连接，并且交换各种数据包，并且能够对接收到的数据包的 SYN/ACK 标志进行分析来猜测操作系统的类型。在被动方式中，Sprint 仅是侦听来自于目标计算机的数据包，并且执行同样的 SYN/ACK 标志分析。除了猜测操作系统，Sprint 同时也能够给出正常的开机运行时间信息。除此之外，Sprint 还能运行复杂的标志抓取功能来发掘更多的系统信息。

（3）Xprobe2 向目标计算机发送特定的 ICMP 或 TCP 数据包，并分析计算机的响应。Xprobe2 不需要首先扫描目标计算机的端口。比起 Nmap 和以主动形式运行的 Sprint，端口扫描功能的缺失以及 ICMP 数据包的使用在计算机上引起了一定的干扰。Xprobe2 同样使用指纹矩阵的方法来代替线性方法，通过使用指纹矩阵能够产生“近似匹配”。当其他的工具返回检测失败的时候，Xprobe2 却能够做出一个积极的响应。

共享扫描

对系统进行扫描时，另一个需要考虑的重要方面就是网络资源的共享。Windows 操作系统允许用户和其他网络用户共享文件夹和打印机等资源。在 Windows 中，这些共享资源被叫做 shares。为了方便远程用户的访问，许多共享资源只有最小程度的保护甚至是没有保护。更糟糕的是，大多数的 Windows 用户已经习惯了访问共享网络资源，并且抵御任何想要限制这种访问的行为。

Windows 使用服务器信息块（SMB）协议提供对共享网络资源的访问。对于 UNIX 系统，Samba 软件提供了同样的资源共享功能。事实上，运行在 UNIX 计算机上的 Samba 允许 Windows 的用户访问 UNIX 计算机上的资源，同时允许 UNIX 的用户访问 Windows 的网络资源。在一个局域网中，Windows 用户使用 UNIX 服务器的共享文件夹和共享打印机是很常见的。

Windows 共享资源功能存在 3 个比较主要的安全漏洞。

（1）共享资源增加了非授权用户获得资源访问权的可能性。用户共享一个资源之后，就必须考虑对资源的访问控制。如果某一个用户的文件夹能够被局域网的所有人访问，攻击者就可以通过攻破局域网的任何一台计算机来获得对资源的访问。在所有安全事故中，攻击者总是会寻找系统中最薄弱的环节进行攻击。

（2）SMB 应用以及 Samba 都包含着一定的缺陷。在著名的漏洞网站上，就有几种 Windows 共享资源的软件漏洞。用户要确保了解最新的软件漏洞，保证所有软件的及时更新。

（3）网络资源共享的漏洞使得攻破一台计算机等同于攻破一组计算机。如果攻击者获得了网络上一台计算机的访问，他就能够将恶意代码引入到共享文件夹中，随后影响整个网络。除非对每个共享资源进行扫描，否则在很长的一段时间内这个问题都不会引起注意。糟糕的是，由于对整个网络进行扫描会耗费很多的时间和资源，很多防病毒软件的默认设置都跳过对共享文件夹和对应驱动机的扫描。

由于 Windows 的网络资源共享存在诸多问题，因此建议慎用这些功能。如果用户必须共享资源，就要确保了解资源的位置，保证每一种资源都是安全的。在 Windows 2003 之前，共享的默认设置是 Everyone-Full Control 权限，也就是说如果用户创建了一个共享，并且没有限制对它的访问，那么所有人都能够对这个共享资源进行读和写。通过在命令提示符下输入 net share，用户可以在 Windows 计算机上查看所有的本地系统共享。共享资源的扫描工具叫做共享扫描，原理是通过向用户网络发送 SMB 数据包检查所有活跃的资源共享。和处理所有的安全事件一样，对共享资源的保护，要确保用户比攻击者了解更多的信息，要限制用户直接泄露的信息数量。要经常对用户网络进行共享扫描，以保证用户使用的所有资源的安全。有多种用于扫描网共享络资源的工具。图 9-3 给出了使用 Nessus 扫描工具得到的某一个网络上的共享资源结果。

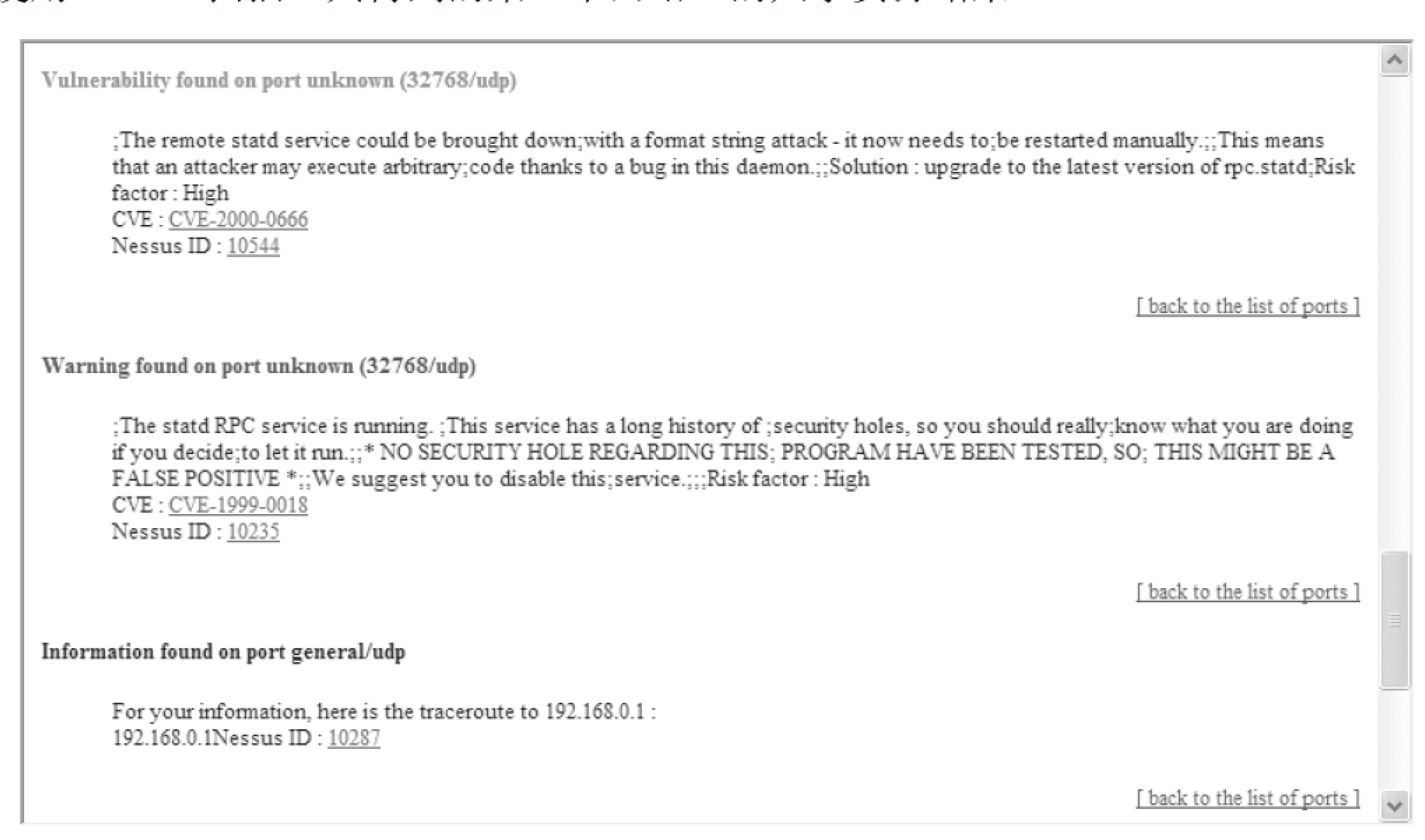


图 9-3　Nessus 得到的某一个网络上的共享资源结果

9.5 Telnet 查询

上文在介绍扫描工具的时候已经对 telnet 命令进行了介绍。默认情况下，telnet 命令使用 23 号端口。如果用户发布一个常规的 telnet 命令，这个命令就会使用 23 号端口和远端主机进行通信，例如下面这种形式：

```
$ telnet 192.168.1.1
```

然而，如果用户在命令行的最后加上特定的端口号，telnet 命令就会使用特定的端口号进行通信，例如下面的形式：

```
$ telnet 192.168.1.1 80
```

这个 telnet 命令试图使用 80 端口与 IP 地址为 192.168.1.1 的主机进行通信。很多侦听 TCP 端口的服务在用户联系它们的时候会给出一些响应。这样使用 telnet 命令就能够在发送数据之前判断是否连接到了正确的服务。因此能够对计算机进行扫描并找到运行的服务。

telnet 被广泛认为是不安全的。用户输入给 telnet 的所有内容都是以明文的形式在网络中传播的。也就是说，通过 telnet 传输的所有文本都可以被第三方截获并读取。如果用户使用 telnet 登录一个远程系统，用户的口令就会以明文的形式传输。为了避免这一安全隐患，用户可以使用安全外壳（SSH）这样的方法替代 telnet。SSH 使用加密的方法降低了用户对话被截获的可能性。

对网络分析而言，telnet 的基本功能能够起到很大的作用，可以使用户直接和远程服务进行交互。熟练使用 telnet 可以帮助用户扫描和分析很多网络漏洞。

9.6 TCP/IP 服务漏洞

最容易被攻击者利用的攻击点就是网络中非必要的和过时的服务。目前大多数的网络服务都使用 TCP/IP 协议为不同系统之间的通信提供接口。尽管统一的标准提供了更多的通信灵活性，但同时也留下了大量的攻击后门。为了增加系统的安全性，用户应该关闭那些非必要的网络服务，原因如下。

（1）非必要的服务为攻击者提供了更多的访问用户系统的入口点。

（2）非必要的服务消耗系统资源，使系统变慢。

（3）非必要的服务很可能使用的是旧版的软件，使得这些服务更容易被攻击。

（4）如果一项服务不是必要的，那么该服务产生的活动就是不连续的。这就更不容易检测到利用该项服务的攻击者的攻击活动。

基于以上原因，用户应当识别出系统所有非必要的服务，关闭或删除它们。这也是使用安全扫描工具的一个重要用途。Nmap 扫描开放的端口，然后在一个本地文件中查找常见的端口服务。如果目标计算机在一个常见端口运行着一个非标准服务，Nmap 就会做出服务不正确的报告。扫描的另一种方式是连接一个端口，然后检测目标计算机发送回来的所有商标信息。图 9-4 给出了 Nessus 扫描工具的一个报告。这个特殊的扫描工

具识别运行在目标计算机上的网络服务。

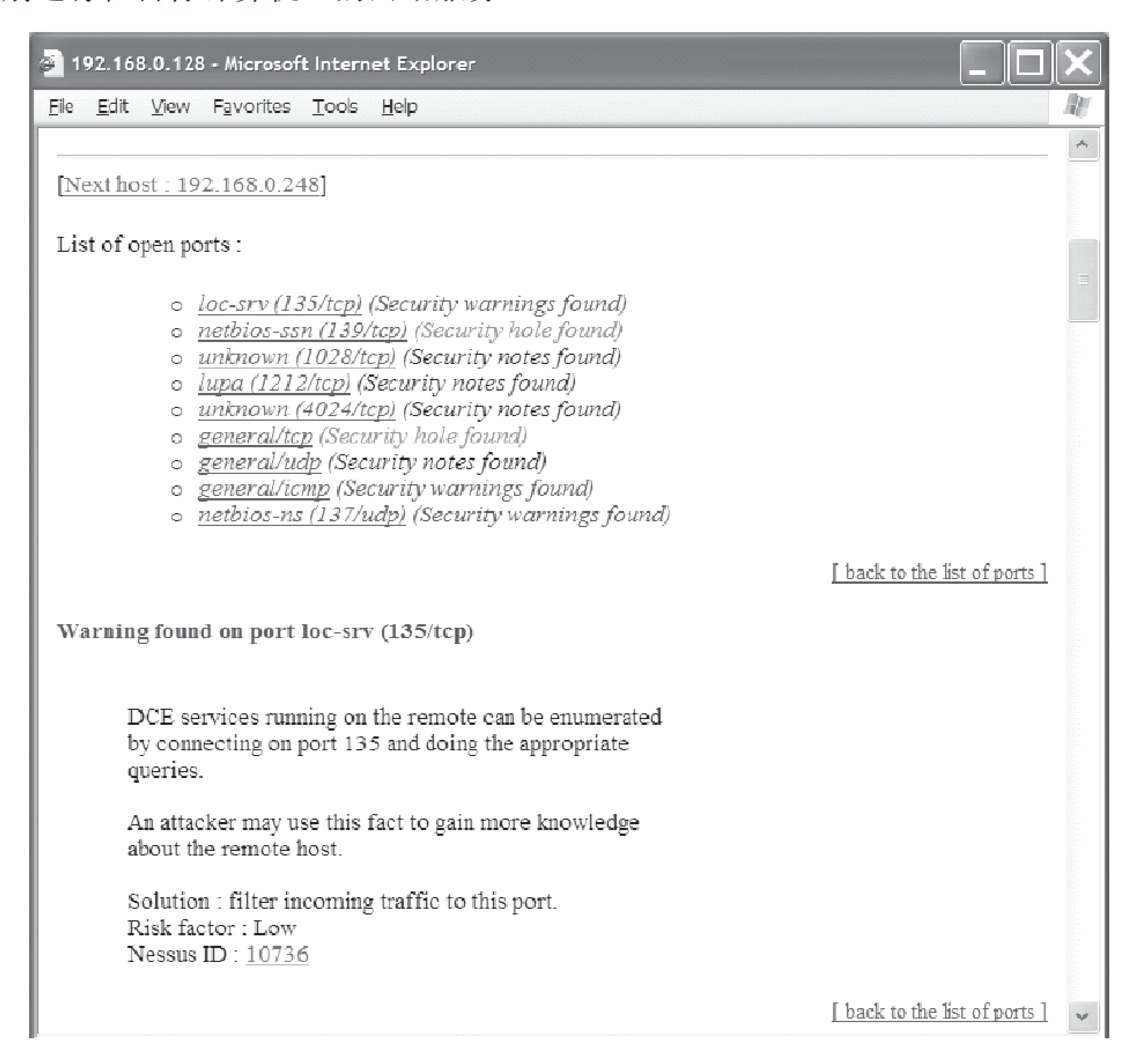


图 9-4 Nessus 的一个报告

很多 TCP/IP 服务存在着漏洞，并且漏洞列表经常变化。用户在进行系统扫描之前，要对扫描软件和漏洞库及时更新。在 Nessus 扫描的案例中，保持产品的更新是很容易的。Nessus 的漏洞扫描工具是模块化编写的，其采取的所有行动都是通过追加程序或外挂程序定义的。为了保持 Nessus 的更新，用户只需要保持每一个插件的更新。Nessus 含有一个命令自动来完成这项功能，下面这个命令就会访问 Nessus 网站（http://www.nessus.org），并且下载所有的更新插件：

```
$ nessus-update-plugins
```

但是插件自动更新并不能免除用户自己进行更新的需要。用户要订阅一个安全更新邮件或经常登录安全网站查找更新信息。附表 A-4 列出了部分安全漏洞邮件列表以及通信订阅页。

9.7 TCP/IP 简单服务

网络服务通过在多台计算机之间传送信息来完成。为了实现信息的顺利传送（尤其

是使用 TCP/IP 协议集的时候），最常使用的策略就是使用端口。端口使得一台计算机上能够运行多个服务，并且能够提供不同的服务和功能。访问网络服务的远程客户端需要知道的就是服务所在的主机名字以及服务侦听的端口号。

标准的 TCP/IP 应用允许的端口号范围从 1 到 65534。其中，0 号到 1023 号被标准服务使用，这些端口又被叫做知名端口号。每个操作系统都有一个文件维持着知名端口列表，以及用户为自己的系统定制的端口的分配情况。这个文件通常叫做 services。表 9-1 列出了在 Windows 和 UNIX 系统中 services 文件的位置。

表 9-1　Windows 和 UNIX 中 services 文件的位置

操作系统	Service 文件位置
Windows	%windir%\System32\Drivers\Etc\Services
UNIX	/etc/services

在一个通用 services 文件中，有很多的条目。图 9-5 给出了来自于红帽 Linux 计算机的 services 文件的一部分。在这个文件中把服务名字（例如 FTP），端口以及使用的协议联系在一起。在 FTP 的例子中，端口号为 21，协议为 TCP。用户应该知道大多数系统支持的常见 TCP/IP 协议，能够帮助用户了解整体的系统知识，同样也能帮助用户识别哪一种服务最可能成为攻击者的目标。

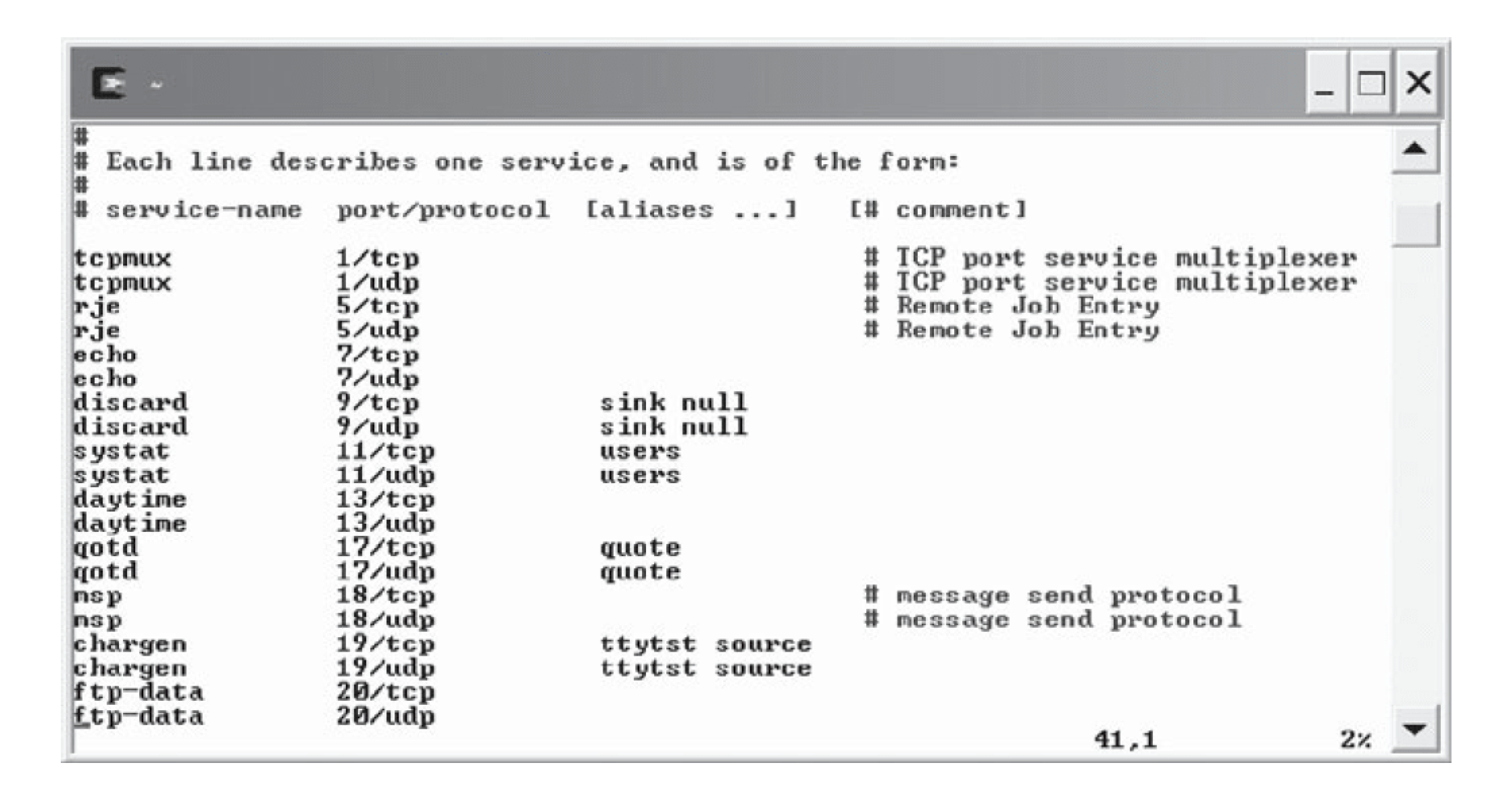


图 9-5　红帽 Linux 计算机 services 文件概况

Windows 操作系统定义了 5 种特殊的服务作为 TCP/IP 简单服务（Simple TCP/IP Services）。事实上，这些服务是为测试的目的而设计的。如果用户不需要这些服务，就可以把它们关闭。如果用户决定关闭在 Windows XP 系统中的这些程序，下面的连接会告诉用户如何操作：

http://www.lokbox.net/SecureXP/simpleTCPIP.asp

对于 Windows 2000 的用户，尝试这个连接：

http://www.lokbox.net/SecureWin2k/simpleTCPIP.asp

关闭 UNIX 系统的服务的步骤会因供应商而不同，可以咨询系统管理员记录来查找关闭不需要的服务所需要的步骤。表 9-2 列出了 Windows 操作系统定义为 TCP/IP 简单服务的 5 种服务。

表 9-2 Windows 操作系统的 5 种简单 TCP/IP 服务

服务名称	端口	描述
CHARGEN（Character Generator）Service	19	侦听 19 号端口，等待连接，之后通过连接倾倒字符
Daytime Server	13	提供系统日期和时间
Discard Server	9	丢弃收到的所有东西
Echo Server	7	对收到的所有通信进行响应
Quote of the Day	17	给出当前日期

9.8 安全扫描总结

为了更有效地对一个系统进行扫描，用户需要下面 5 个方面的要素：目标、权限、过程、耐心和坚持。

（1）对于扫描系统用户必须设定明确的目标。由于会花费较多的时间，因此用户应该做出合理的时间安排。要认识到扫描对于系统安全的重要性。用户目标能够帮助选择扫描工具以及管理项目的方式。如果用户没有合适地定义自己的目标，可能做一些多余的工作。

（2）用户必须获得所需要的权限来对系统进行扫描和评估。如果用户事先没有获得权限，很可能会遇到麻烦。

（3）确定扫描的过程。不要在一开始的时候就进行扫描，要思考一下自己想要扫描的是什么东西。减少扫描的范围能够很大程度地提高扫描的速度。用户还需要决定扫描的入侵程度；选择评估是主动进行还是被动进行；决定评估过程是想秘密进行还是希望高调进行；决定是否计划发动攻击目标的攻击。这些问题是用户计划扫描过程时需要被考虑的因素。用户需要花时间制定详细的计划，以避免漏掉重要的步骤。

（4）最后的因素是相关联的。用户对目标进行彻底的评估必须有足够的耐心。很多测试都是重复进行的，并且速度很慢。但如果测试是必须的，就必须坚决执行。制定一个周密详尽的计划，然后耐心地实施，在完成之前不要停下来。很多时候，扫描过程会受到时间和状态很大的影响。某个星期执行的扫描结果很可能和接下来的一个星期进行的相似的扫描是不相同的。尽可能将所有必须的评估放在一起执行。

建议用户使用 Nessus 漏洞扫描工具。Nessus 的网站地址是 http://www.nessus.org，此网站提供了 Nessus 扫描程序、文档材料以及如何使用 Nessus 的简单教程。不论选择哪种工具，都要学会如何使用它们。然后依照这 5 个步骤，用户就能够执行高效的系统扫描并获得第一手信息来增加系统的安全。

习　　题

一、选择题

1. Telnet 命令的默认端口号是什么？（　　）

A. 80　　　　B. 8080

C. 21　　　　D. 23

2. 在 Windows 操作系统中，端口号 9 提供什么服务？（　　）

A. 给出当前日期

B. 丢弃收到的所有东西

C. 对受到的所有通信进行响应

D. 提供系统日期和时间

二、简答题

1. 什么是安全扫描，其基本步骤是什么？

2. Windows 的共享资源存在哪些安全漏洞，该如何防范？

3. 操作系统指纹识别有哪些方法和常见工具？

课后实践与思考

网络安全扫描器（X-Scan）的使用

一、X-Scan 简介

X-Scan 采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能。扫描内容包括远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等 20 多个大类。对于多数已知漏洞，给出了相应的漏洞描述、解决方案及详细描述链接。

1．X-Scan 图形界面（见图 9-6）

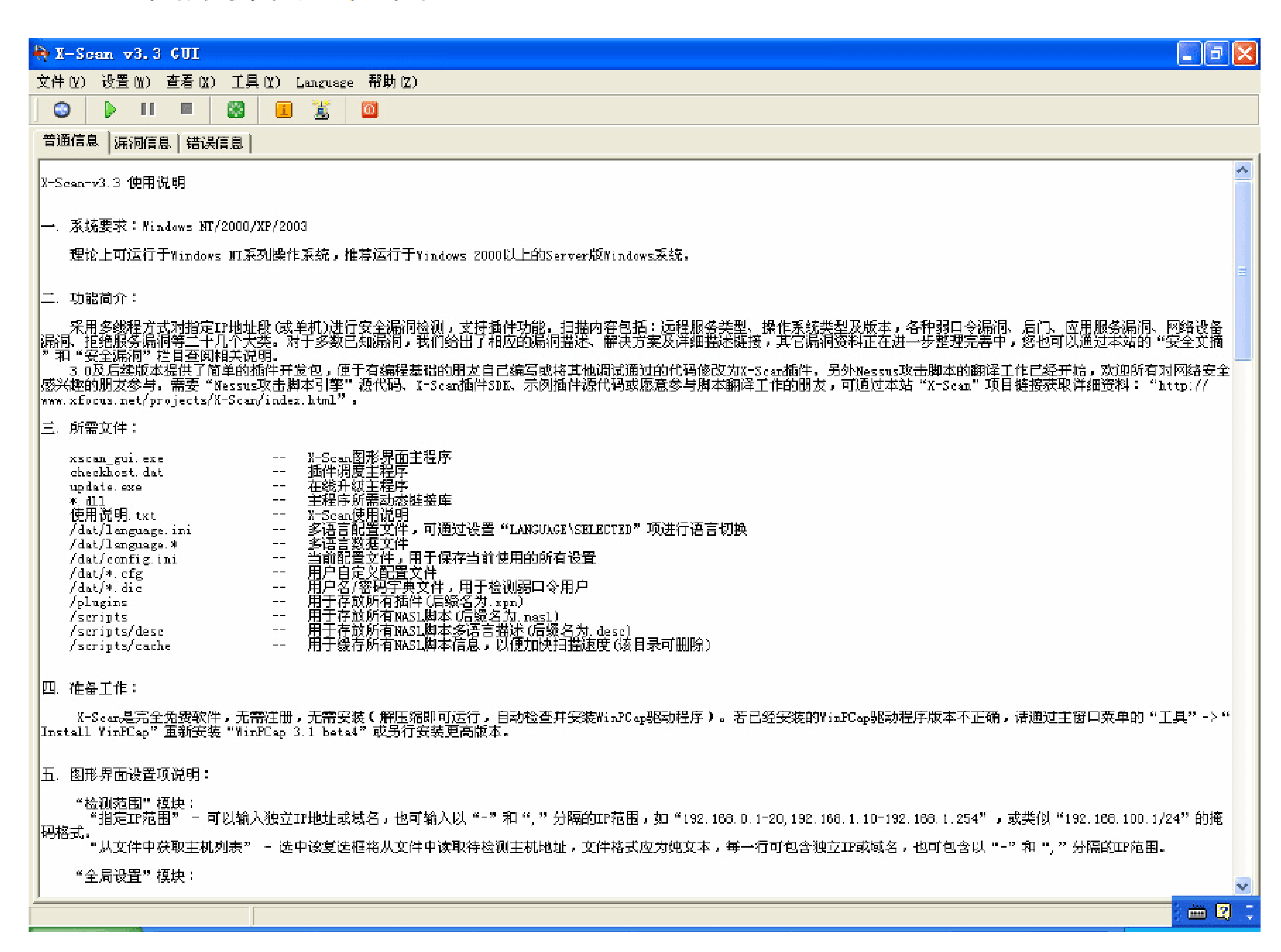


图 9-6　X-Scan 图形界面

2．扫描参数

选择“设置”→“扫描参数”命令，打开如图 9-7 所示的窗口。

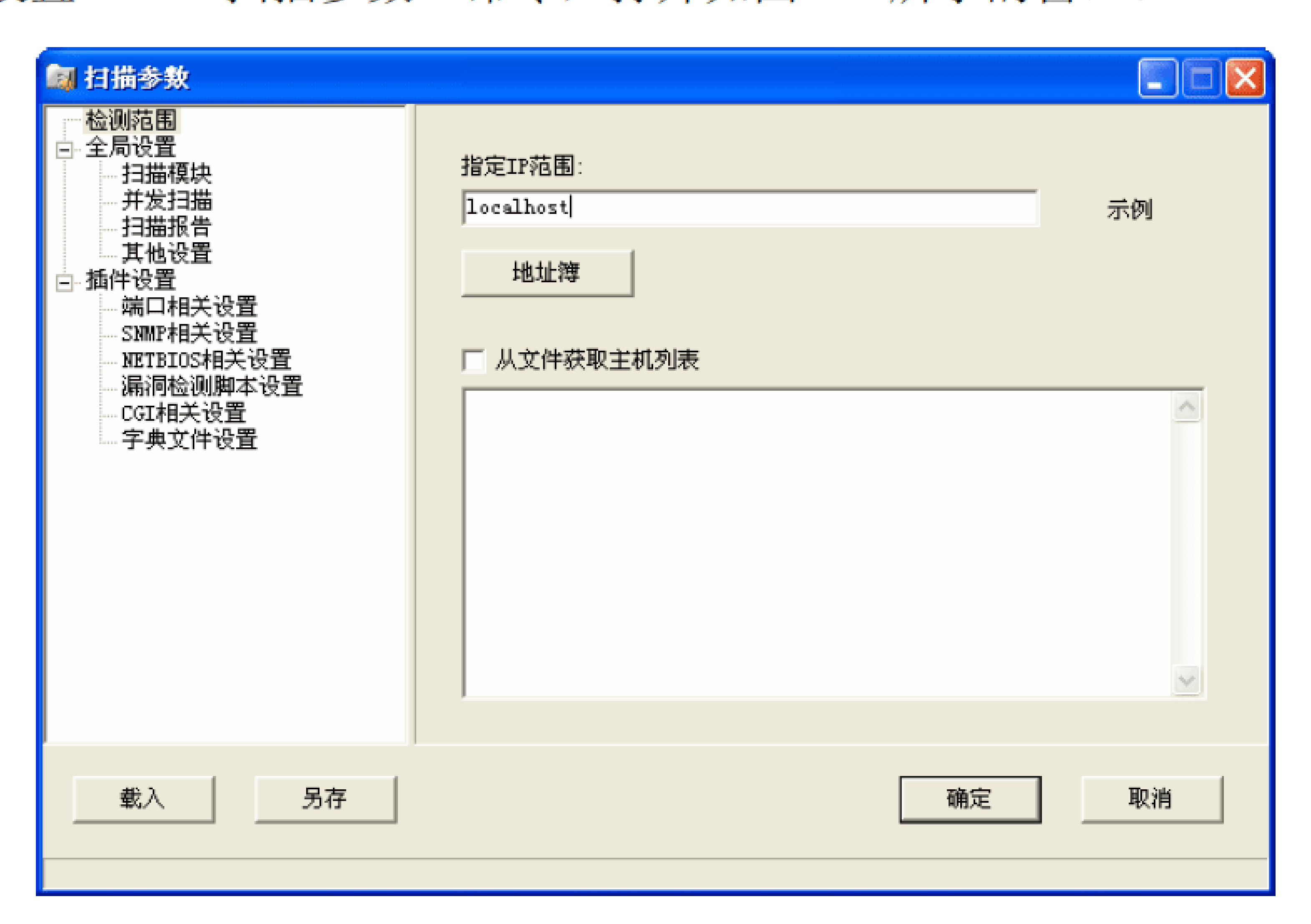


图 9-7　“扫描参数”窗口

选择“检测范围”模块，如图 9-8 所示，在“指定 IP 范围”输入要扫描的 IP 地址范围，如：“192.168.36.1-255，192.168.3.25-192.168.3.80”。

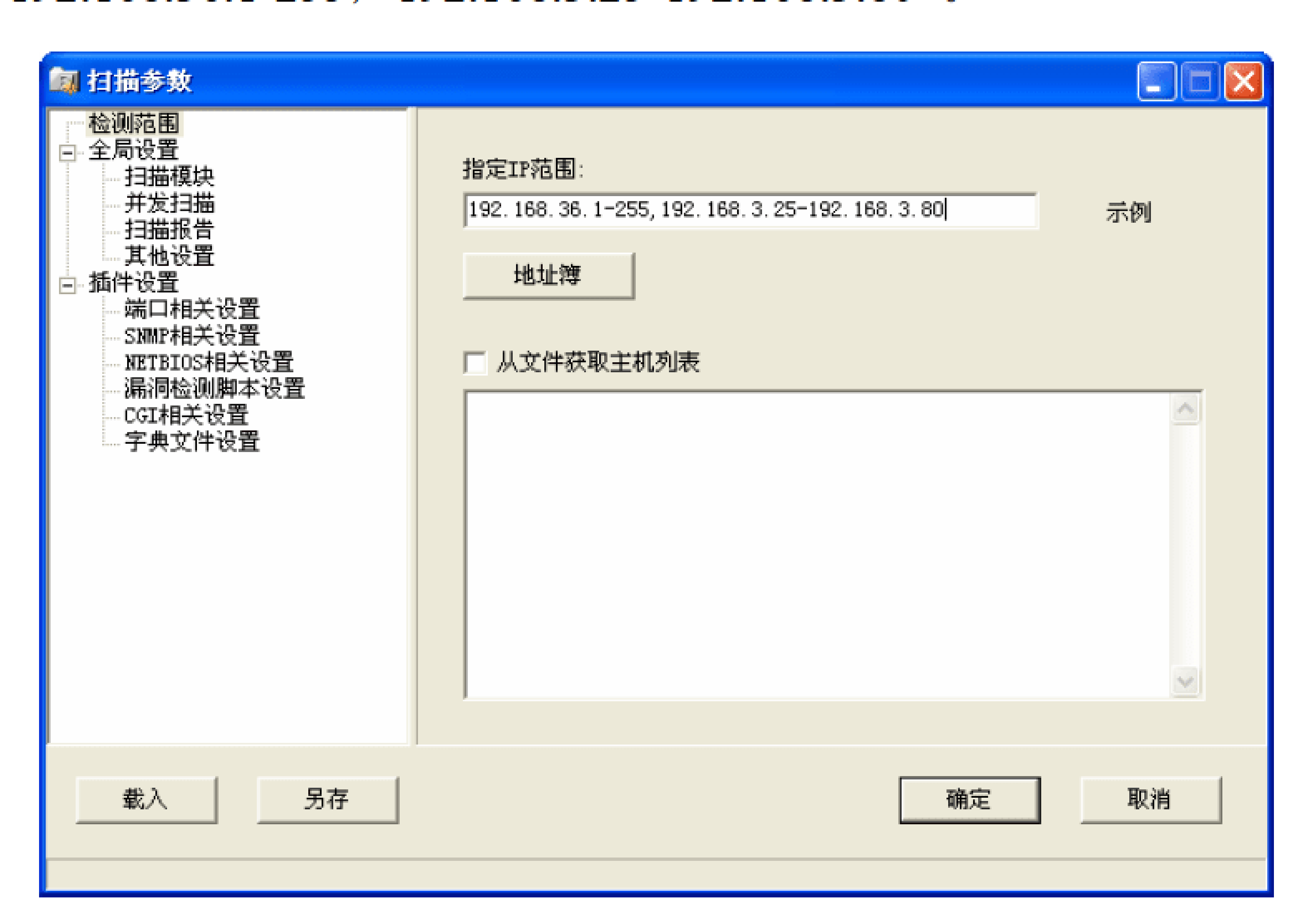


图 9-8　扫描参数设置

3．设置“全局设置”模块

（1）“扫描模块”项：选择本次扫描要加载的插件，如图 9-9 所示。

（2）“并发扫描”项：设置并发扫描的主机和并发线程数，也可以单独为每个主机的各个插件设置最大线程数，如图 9-10 所示。

（3）“扫描报告”项：在此模块下可设置扫描后生成的报告名和格式，扫描报告格式有 TXT、HTML、XML 3 种格式，如图 9-11 所示。

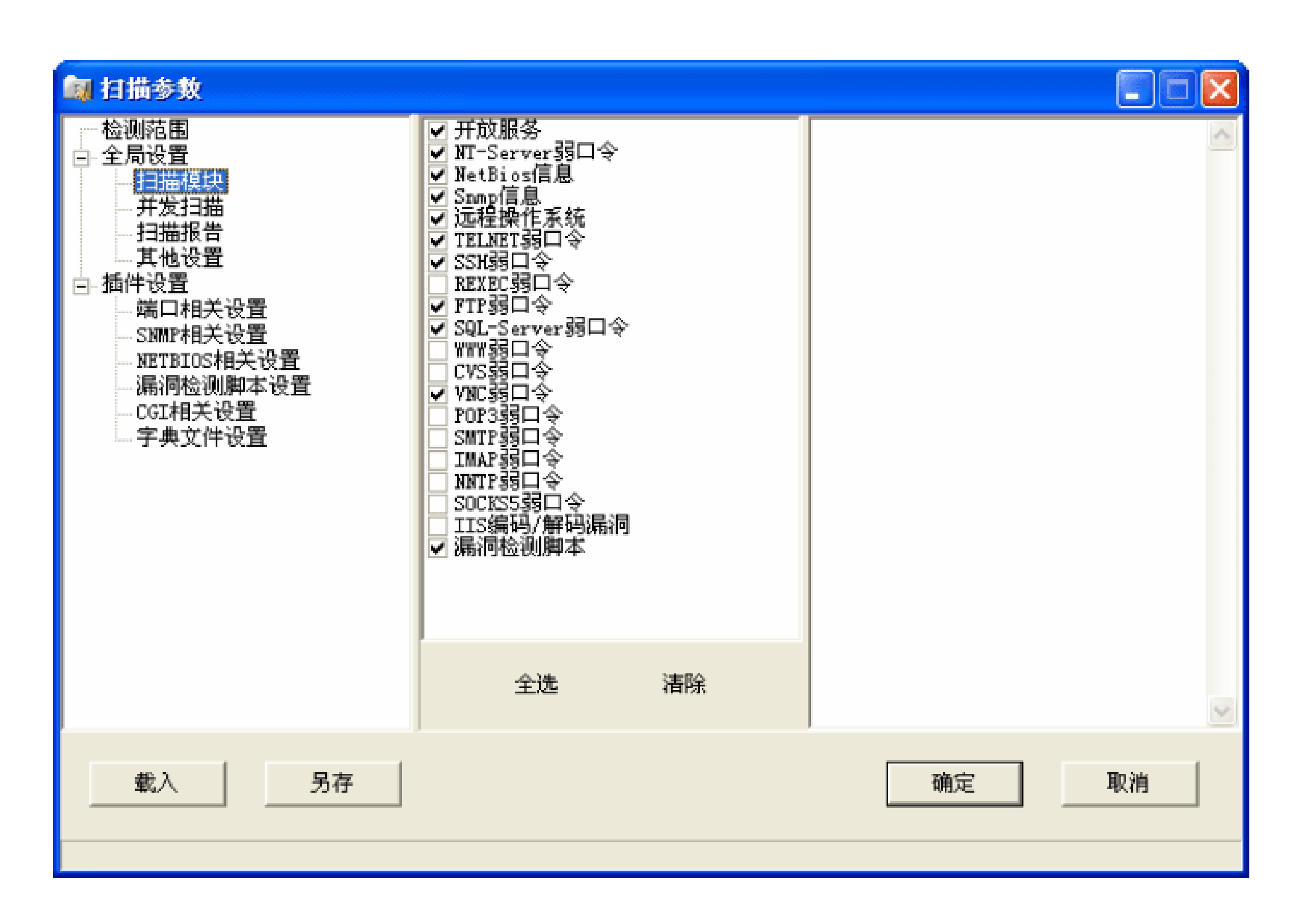


图 9-9　选择扫描模块

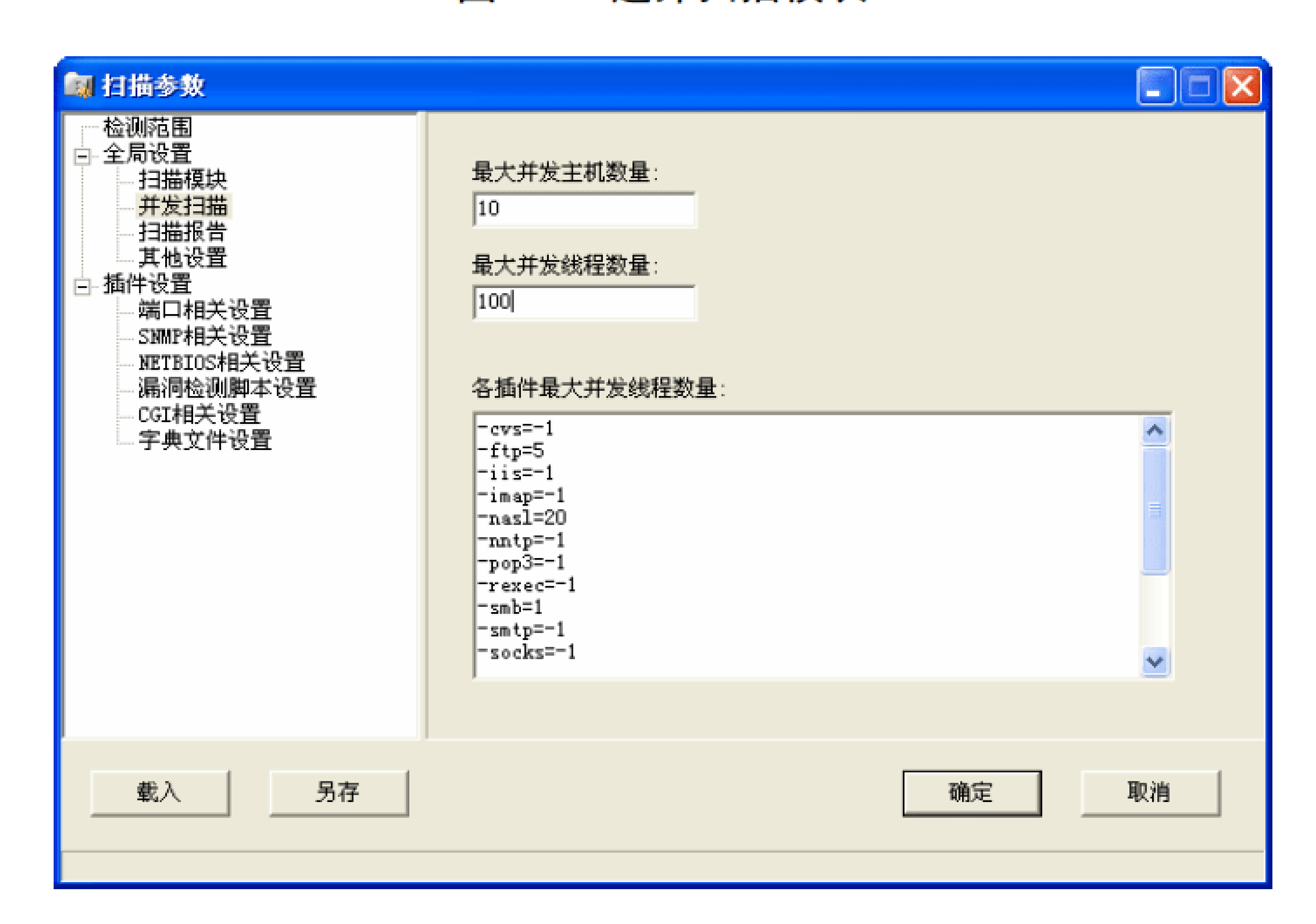


图 9-10　并发扫描设置

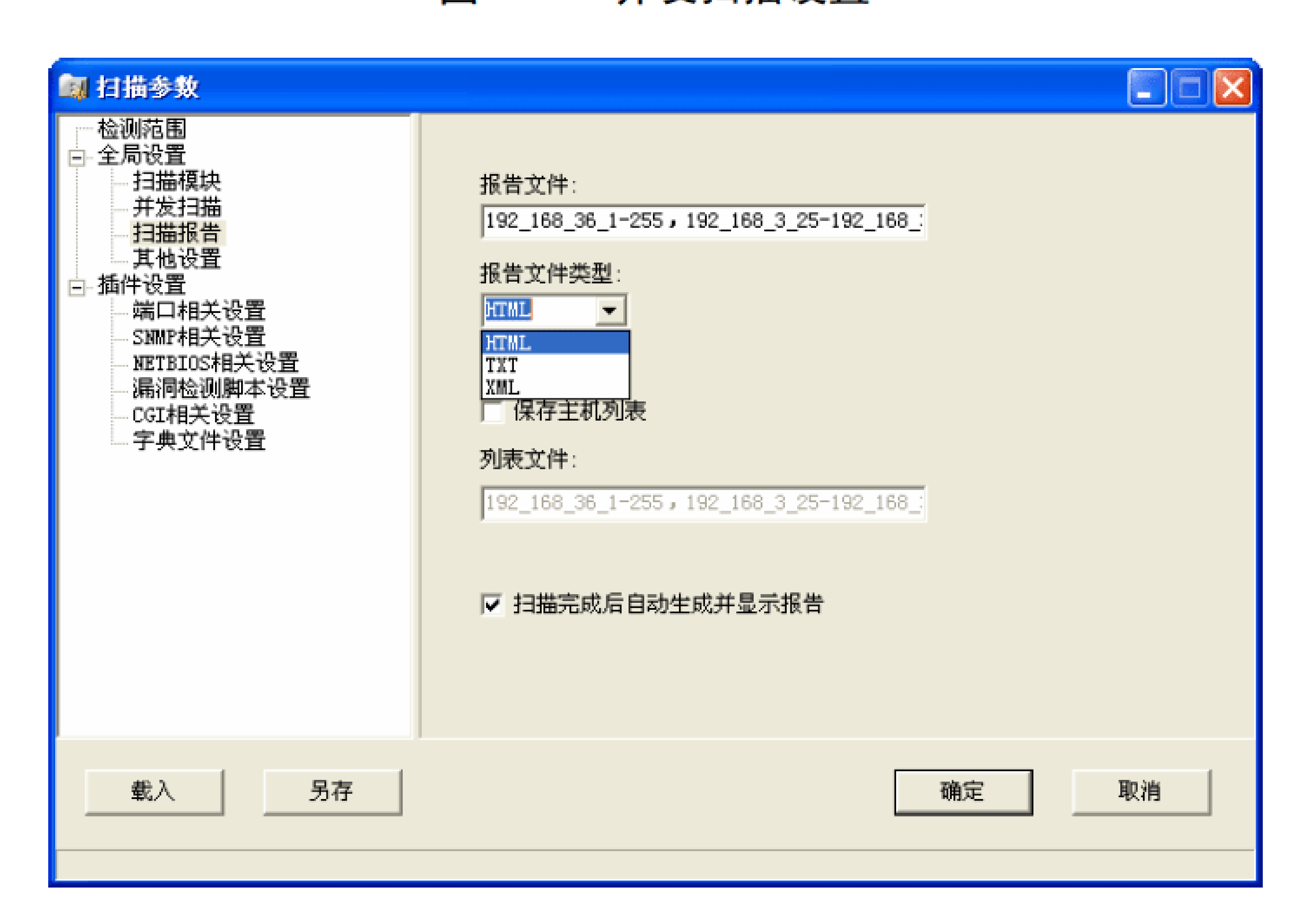


图 9-11　扫描报告设置

（4）“其他设置”项：使用默认选项，如图 9-12 所示。

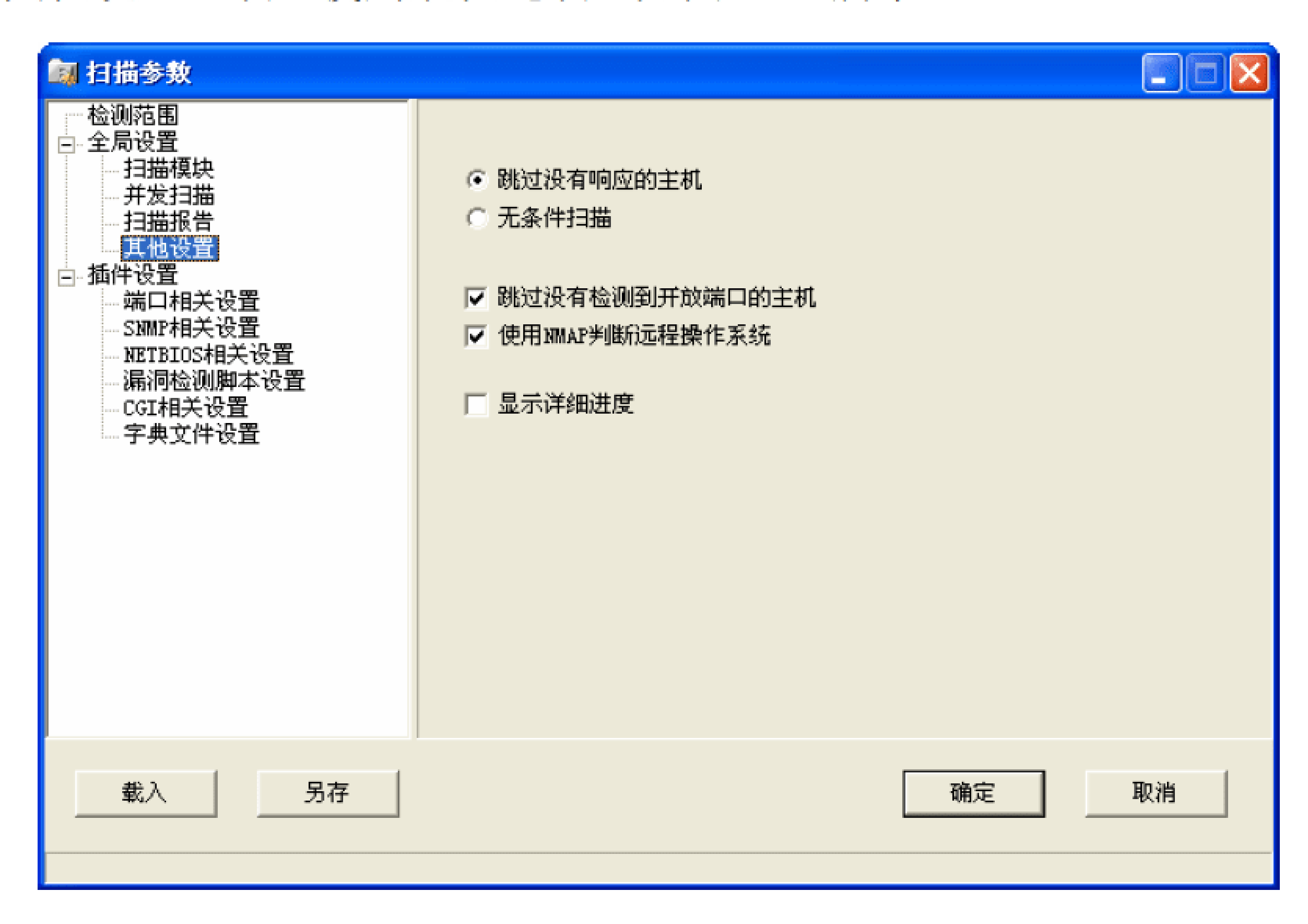


图 9-12　其他设置

4．设置“插件设置”模块

在“插件设置”模块中使用默认设置。

（1）端口相关设置：此模块中默认检测方式为 TCP，也可选用 SYN，如图 9-13 所示。

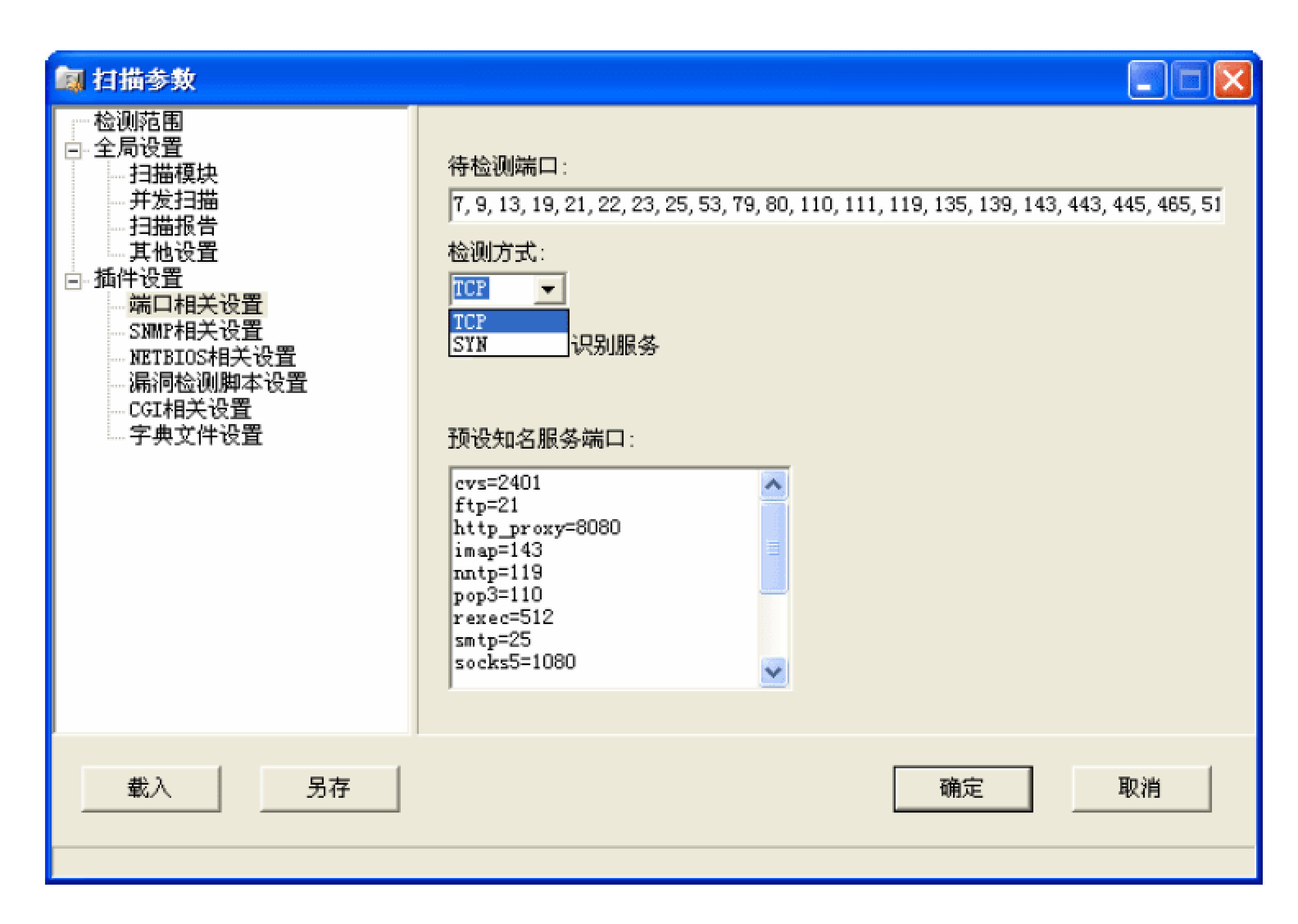


图 9-13　端口相关设置

（2）SNMP 相关设置如图 9-14 所示。

（3）NETBIOS 相关设置如图 9-15 所示。

（4）漏洞检测脚本设置如图 9-16 所示。

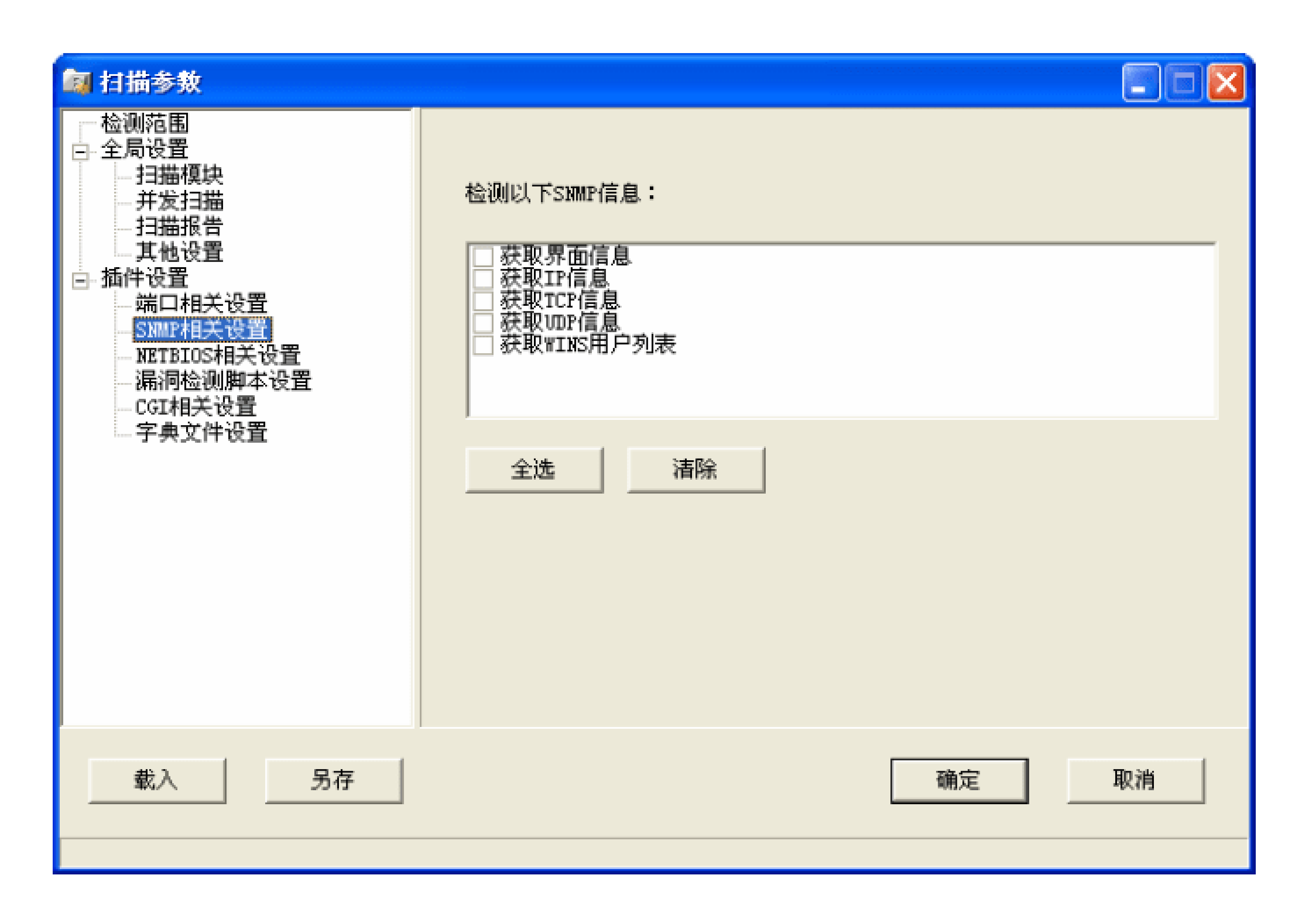


图 9-14　SNMP 相关设置

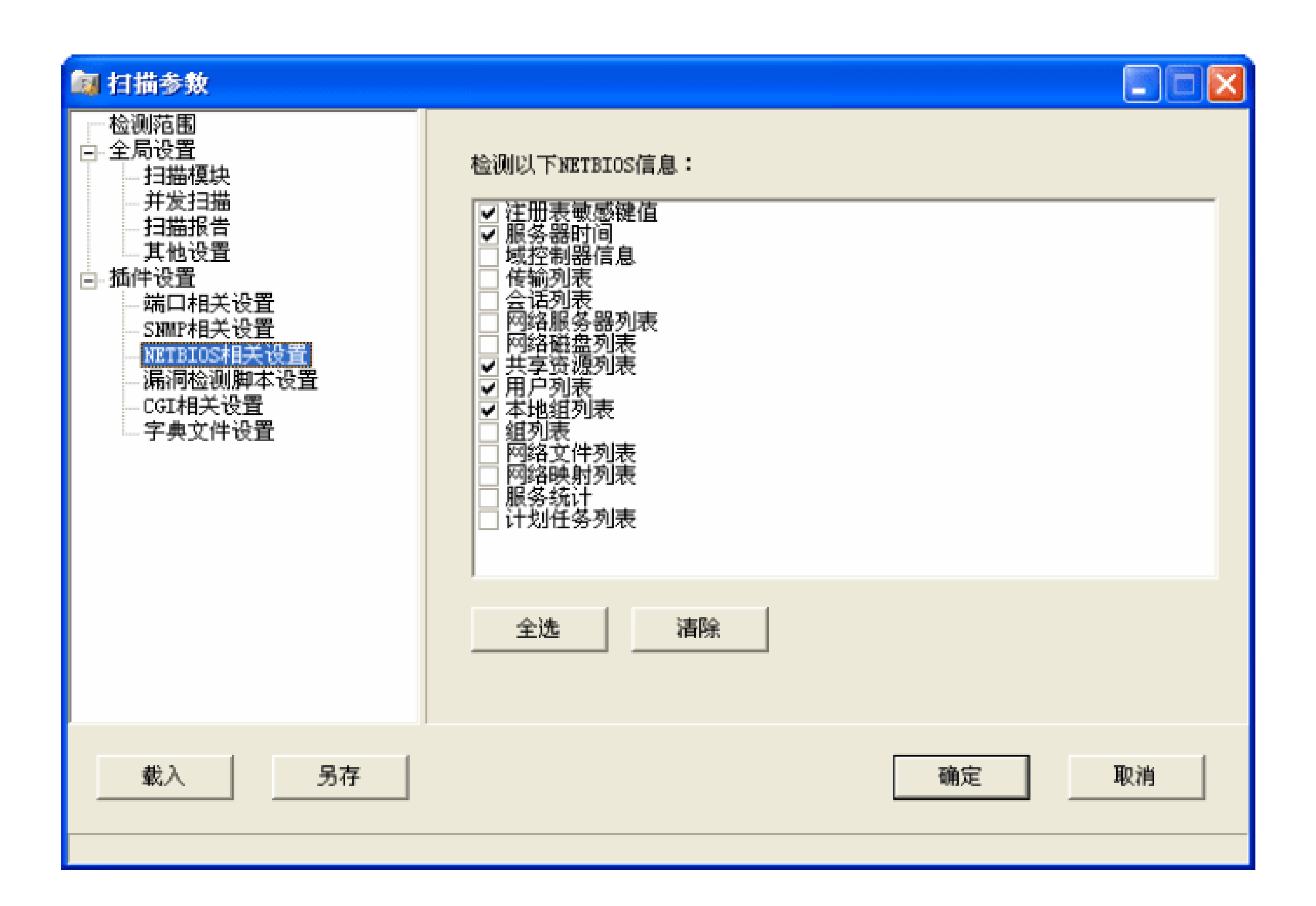


图 9-15　NETBIOS 相关设置

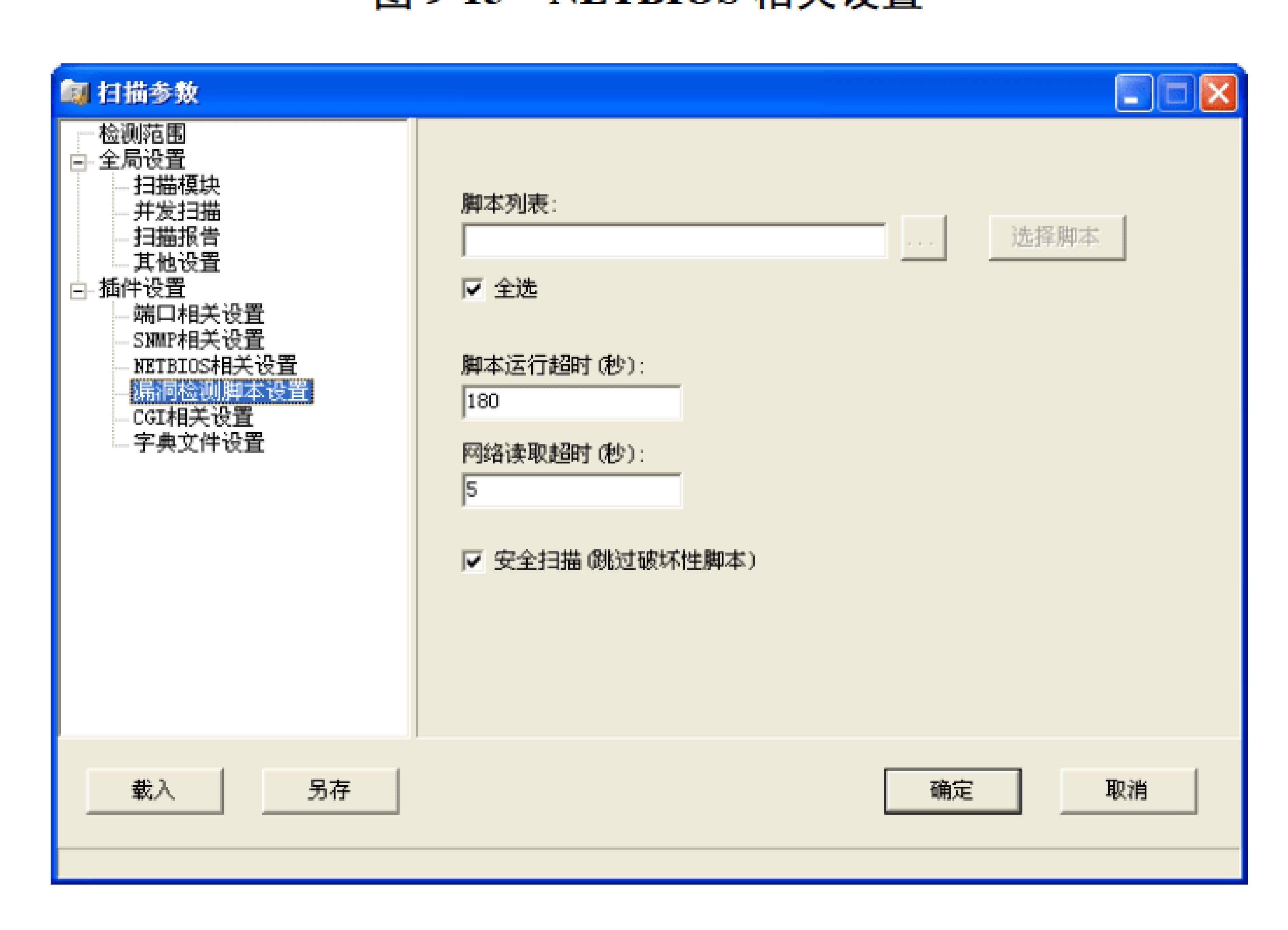


图 9-16　漏洞检测脚本设置

（5）CGI 相关设置如图 9-17 所示。

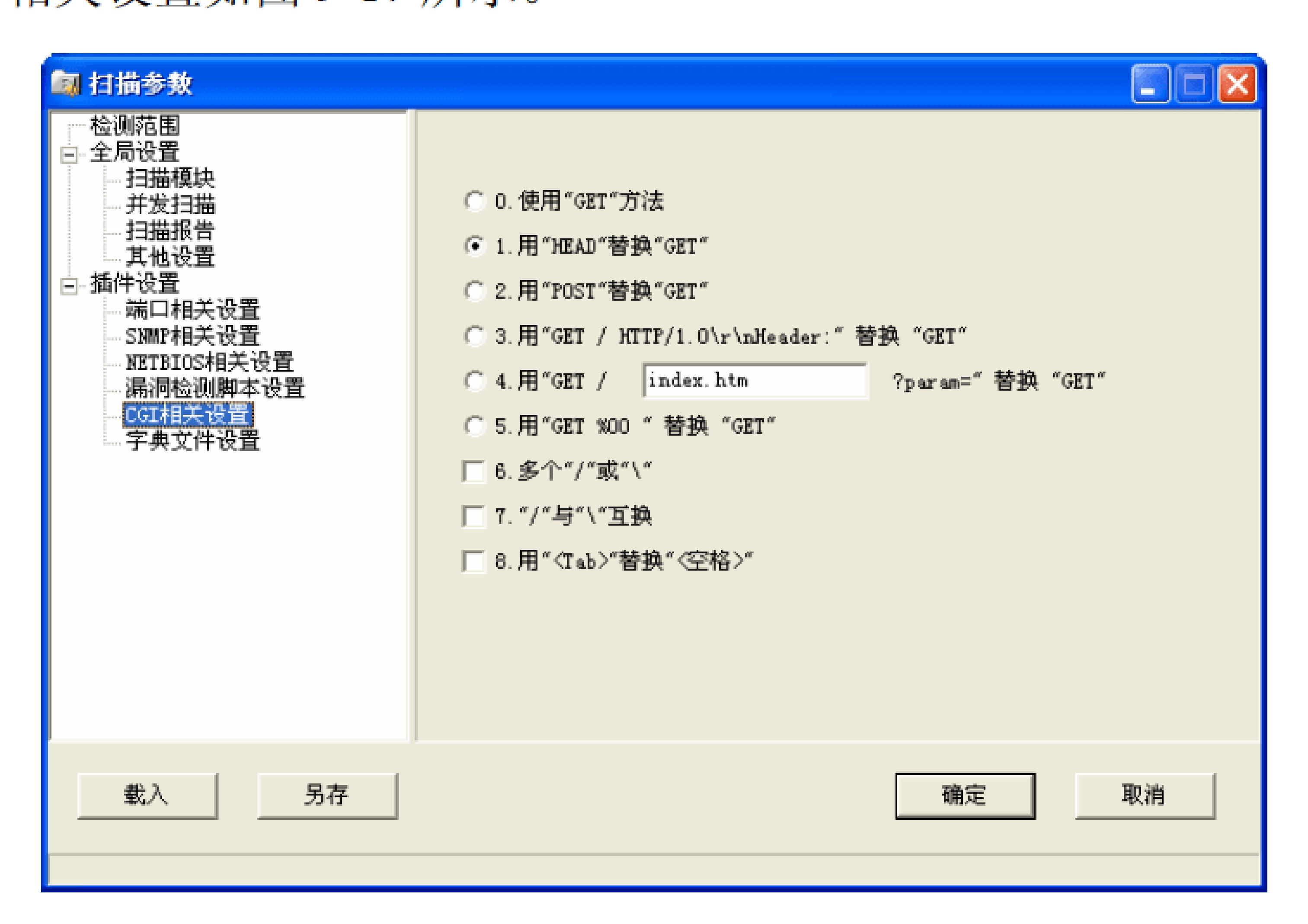


图 9-17　CGI 相关设置

（6）字典文件设置如图 9-18 所示。

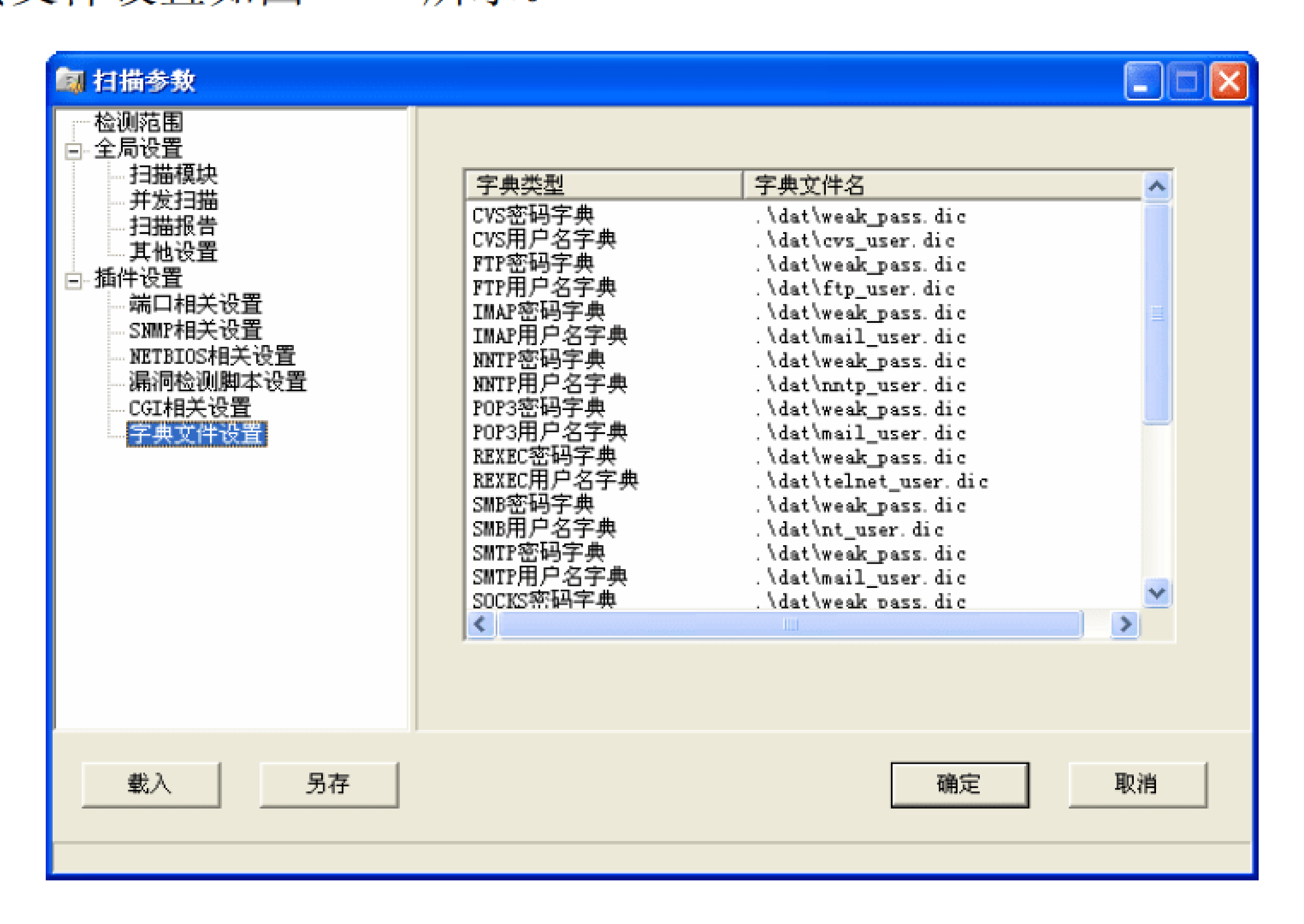
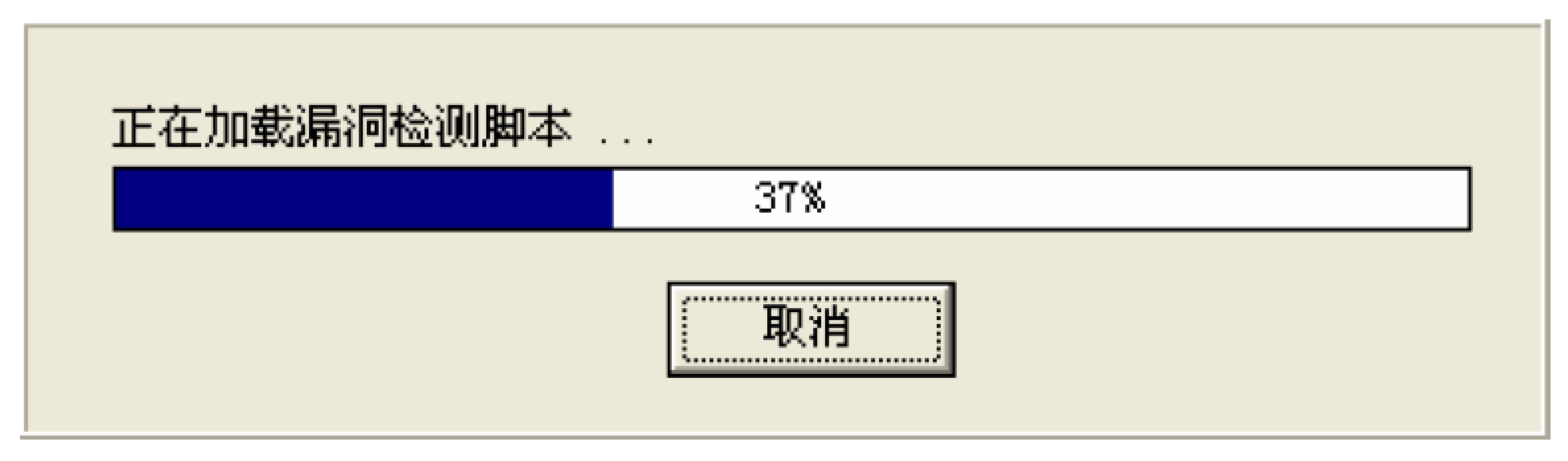


图 9-18　字典文件设置

设置完成后，单击"确定"按钮。

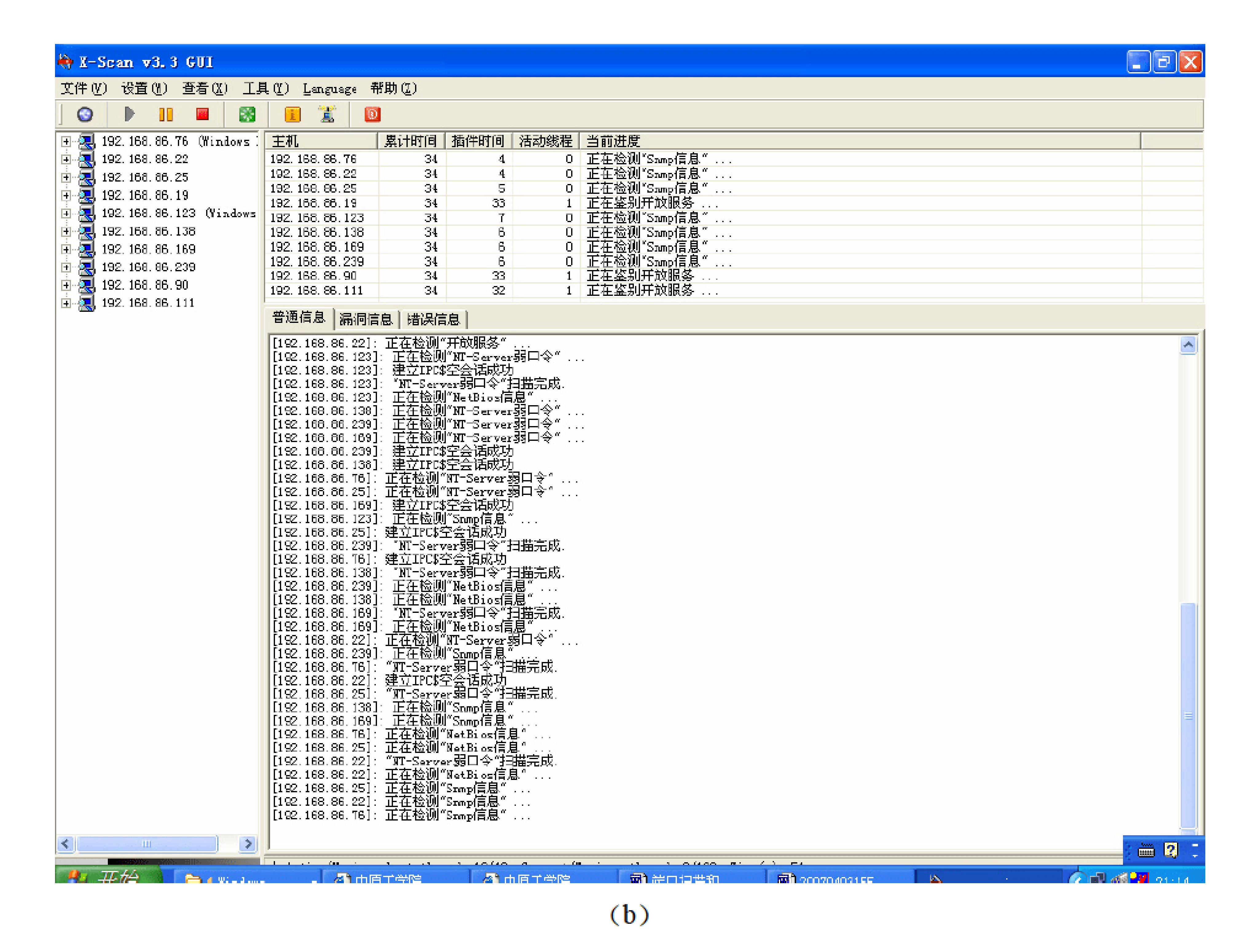
5．开始扫描

选择"文件"→"开始扫描"命令，扫描过程如图 9-19 所示。



（a）





（b）

图 9-19 开始扫描

6．查看扫描报告

选择“查看”→“检测报告”命令，结果如图 9-20 所示。

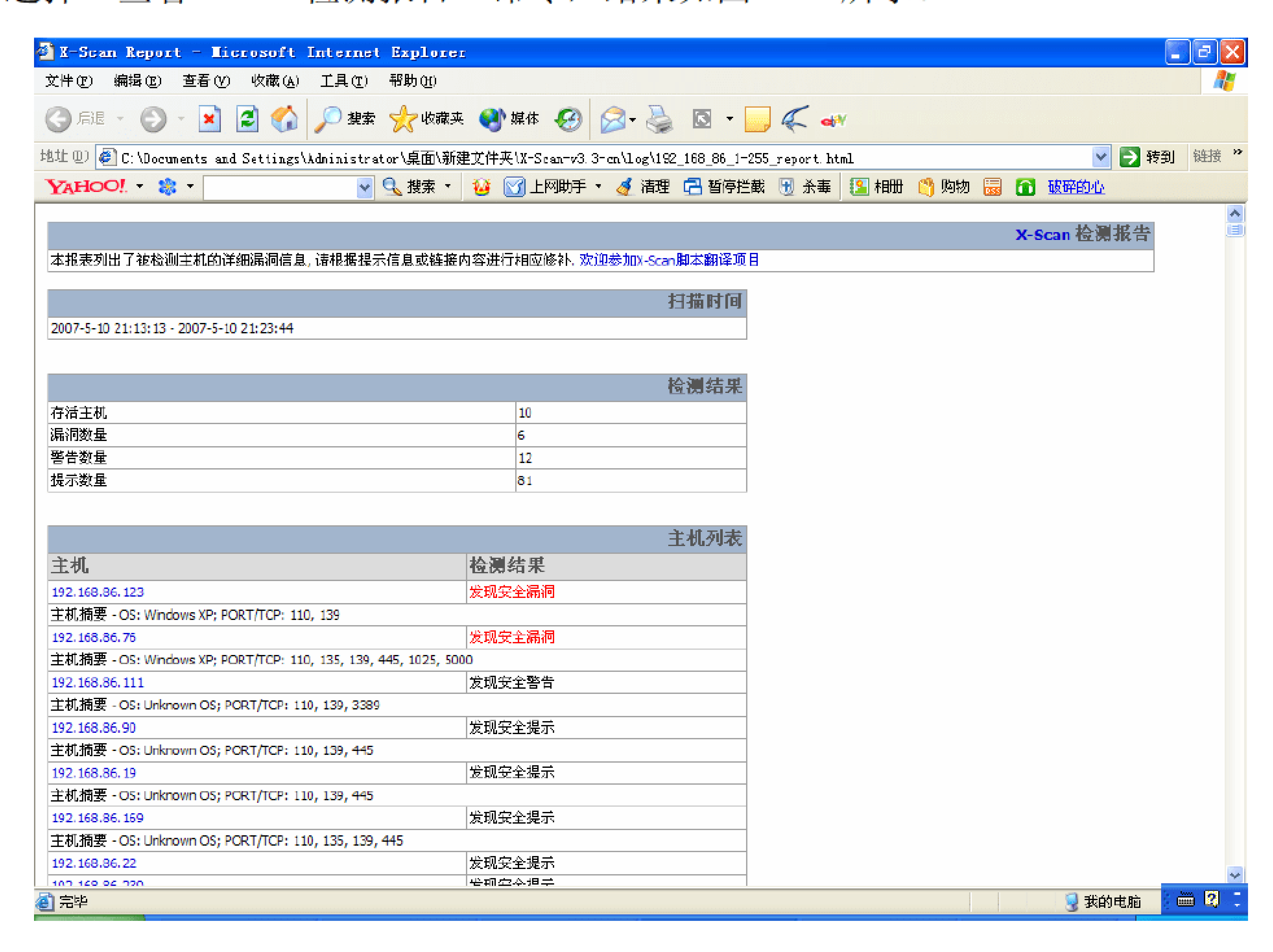


图 9-20 扫描报告

二、X-Scan 操作实例

1．扫描远程主机是否存在 NT 弱口令（获取管理员权限）

（1）打开 X-Scan，在“设置”下拉菜单中选择“扫描参数”命令，打开扫描参数设置窗口。在指定 IP 范围的输入框输入希望扫描的 IP 地址段。本例中将对局域网进行扫描，输入的 IP 段为 192.168.86.1 至 192.168.86.254，如图 9-21 所示。

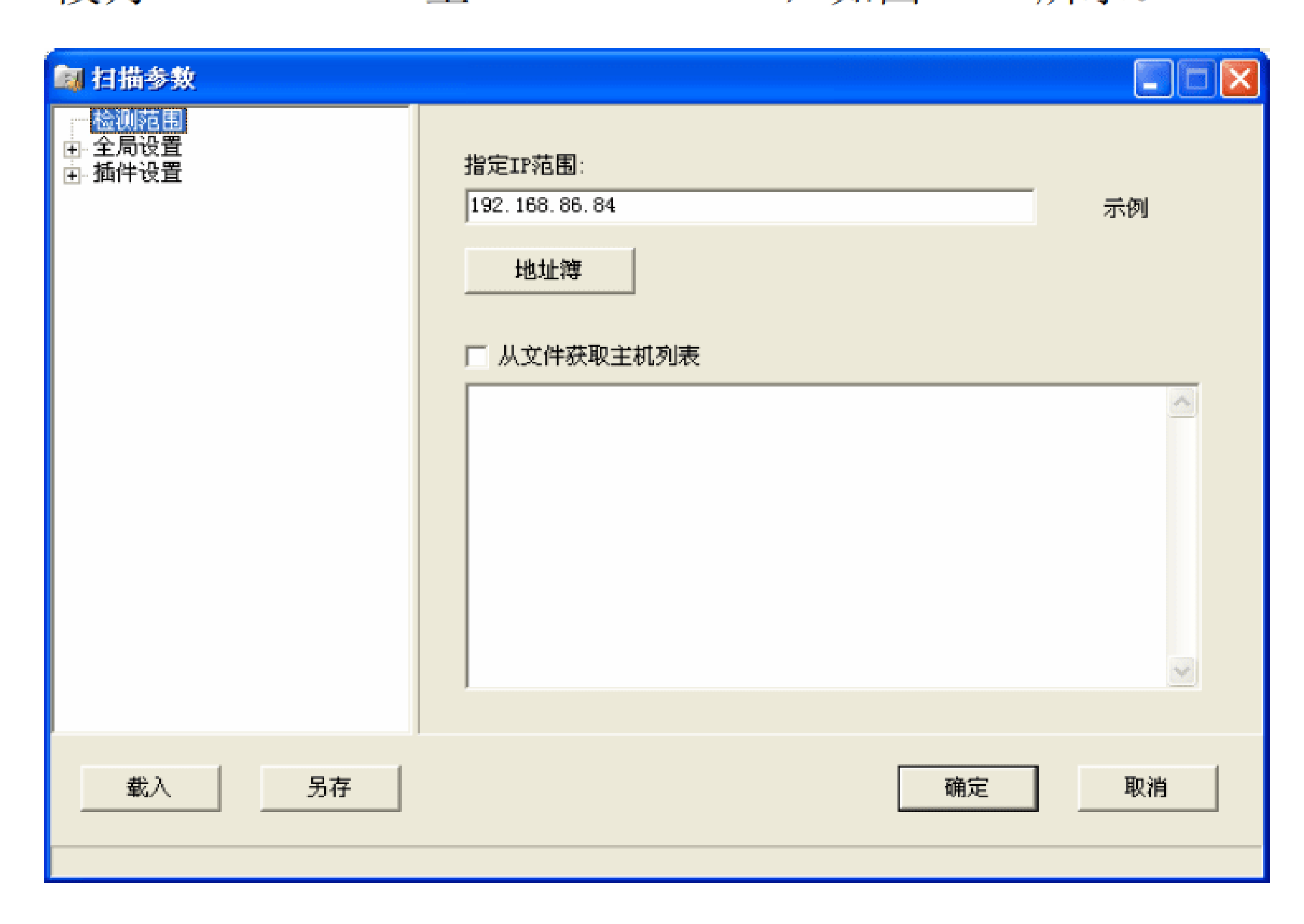


图 9-21　检测范围设置

（2）单击“全局设置”项，在扫描模块中选择 NT-Server 弱口令，如图 9-22 所示。

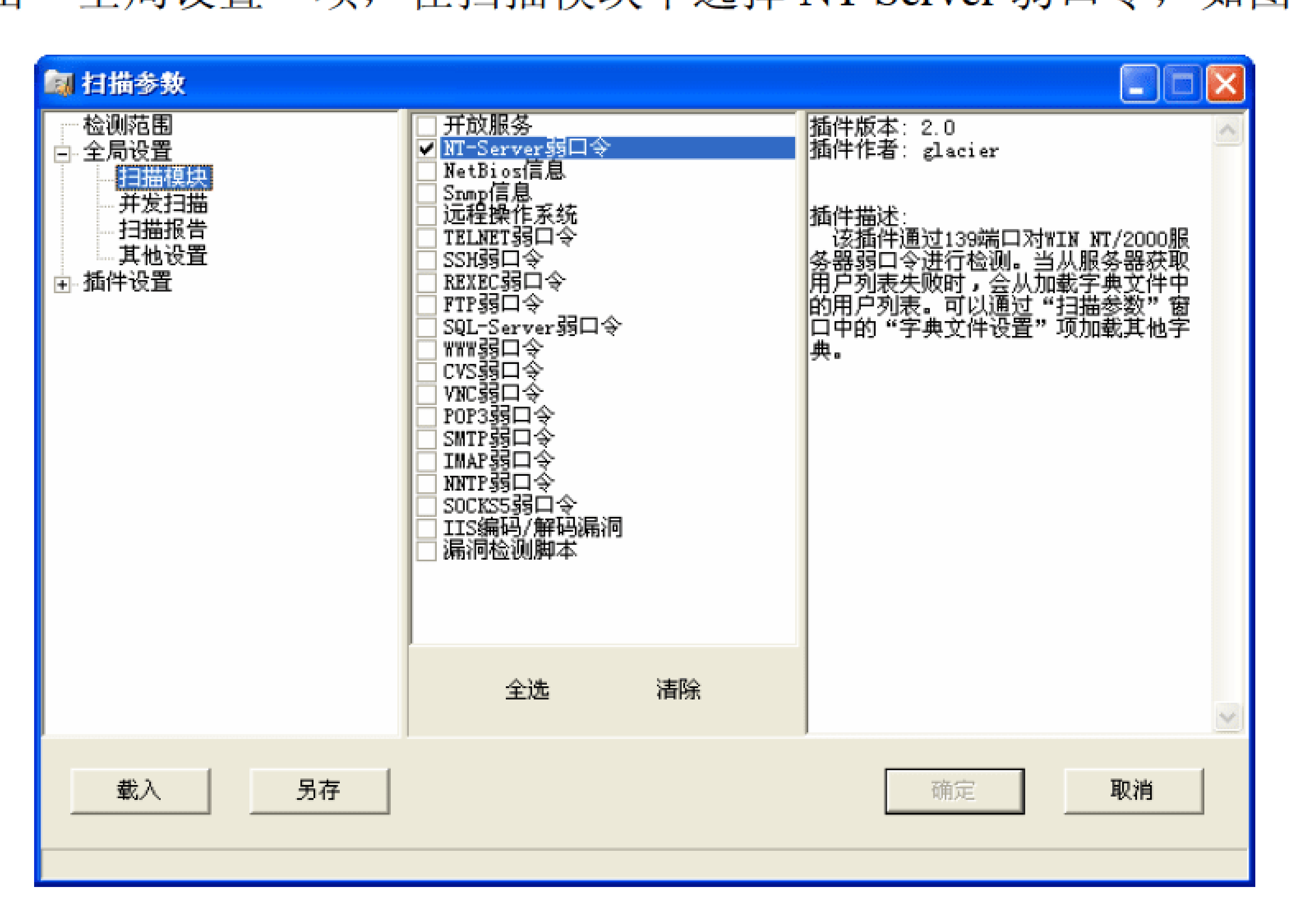


图 9-22　扫描模块设置

（3）单击“确定”按钮后，回到主界面，单击开始图标进行扫描。扫描结果如图 9-23 所示。

IP 地址为 192.168.86.84 的主机存在 NT-Server 弱口令。

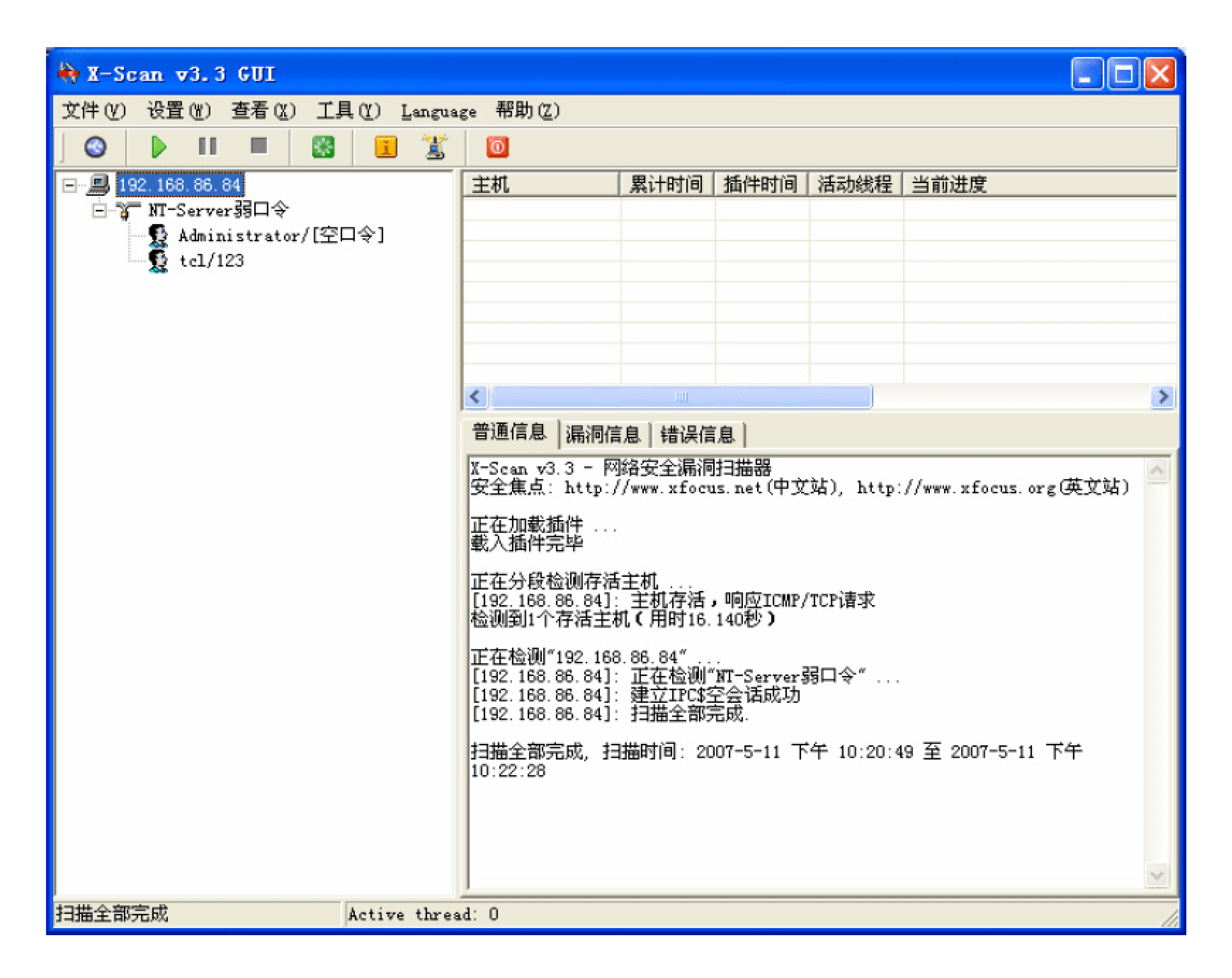


图 9-23　扫描结果

（4）生成扫描报告，如图 9-24 所示。

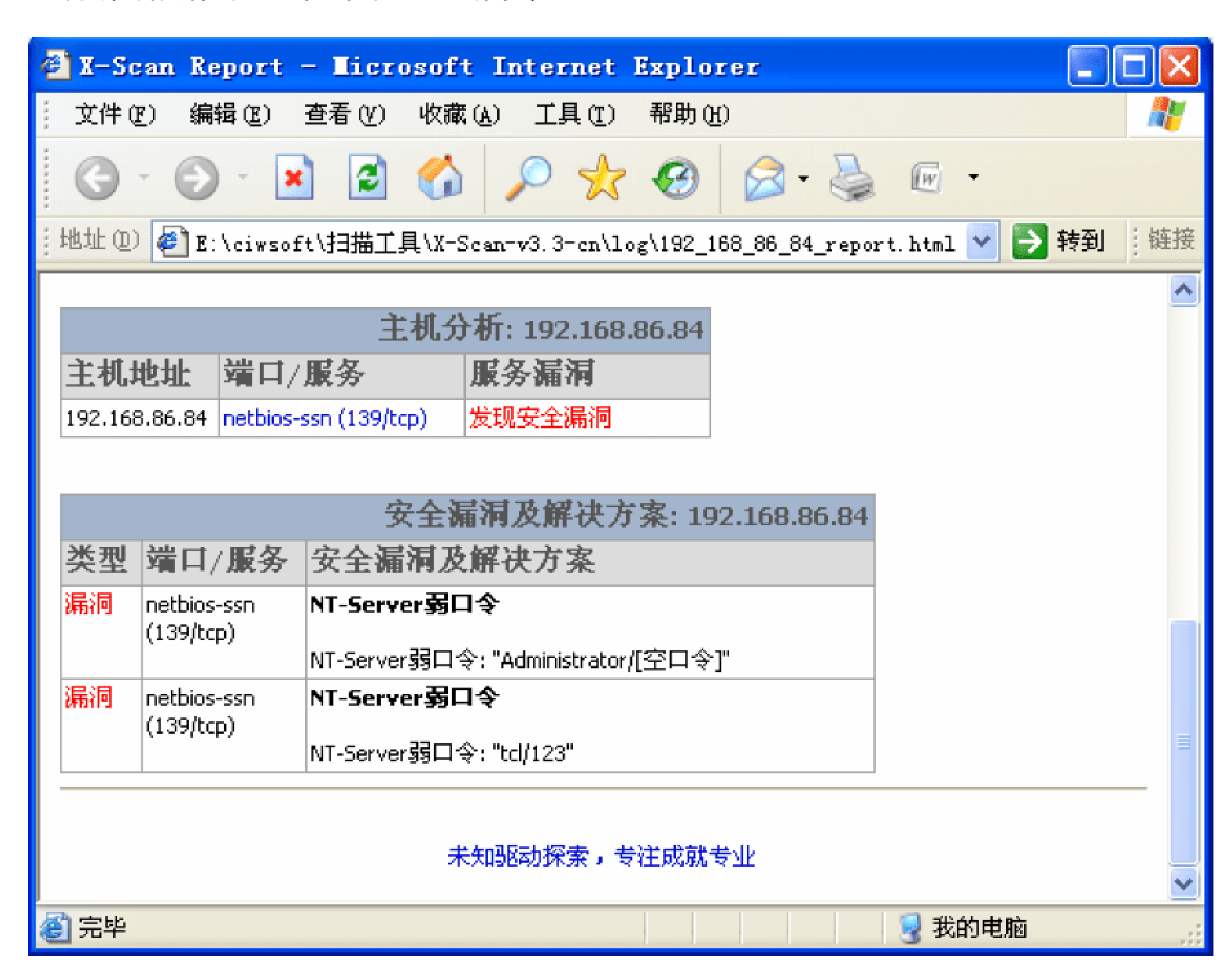


图 9-24　扫描报告

2．在 DameWare 中添加远程主机

（1）单击“开始”→“程序”→DameWare NT Utilities→Dame Ware NT Utilities 命令，打开 DameWare 主界面，如图 9-25 所示。

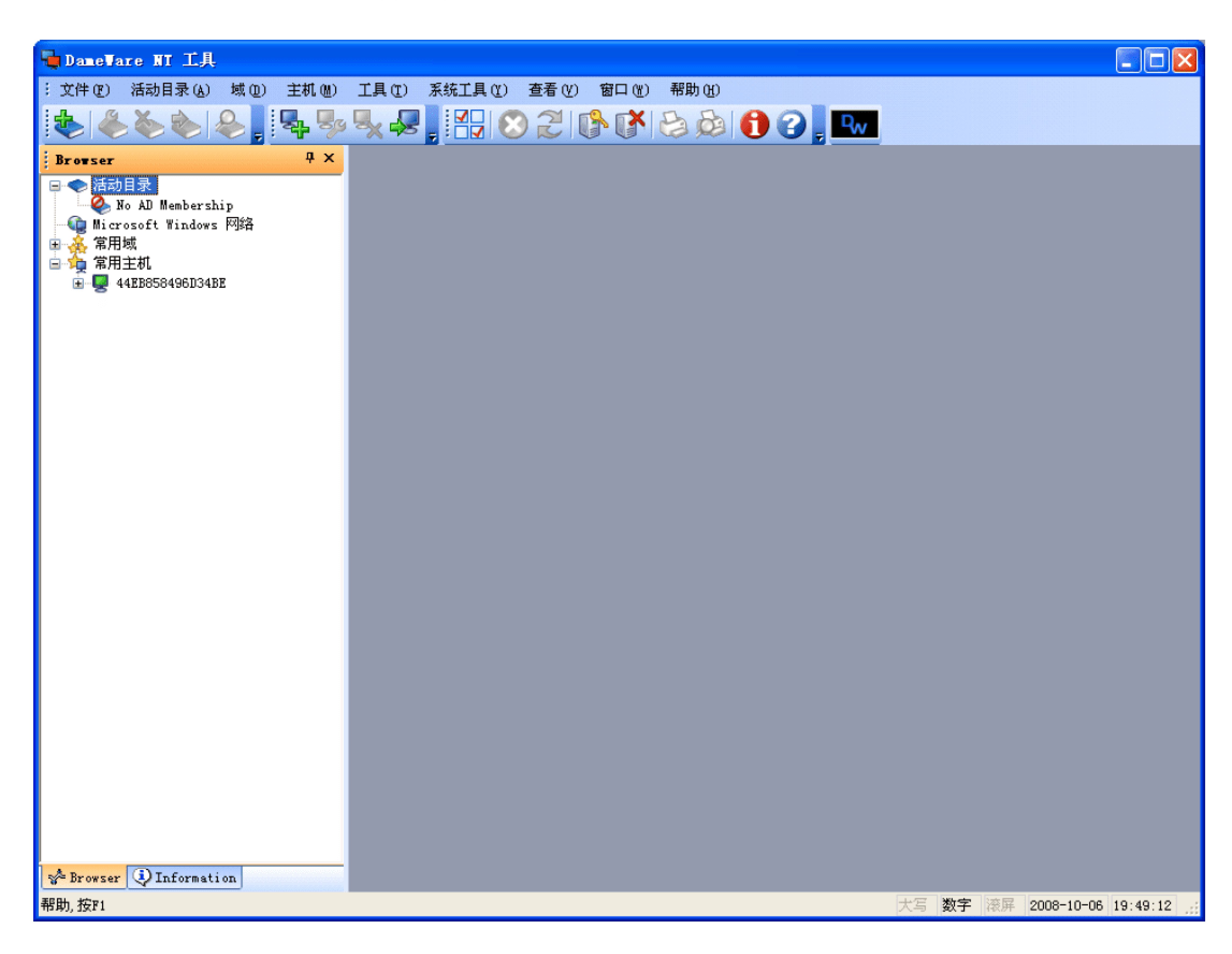


图 9-25 DameWare 主界面

（2）然后单击主界面左上角的图标，接着在如图 9-26 所示的界面添加主机。

（3）添加主机 IP 地址，如图 9-27 所示。

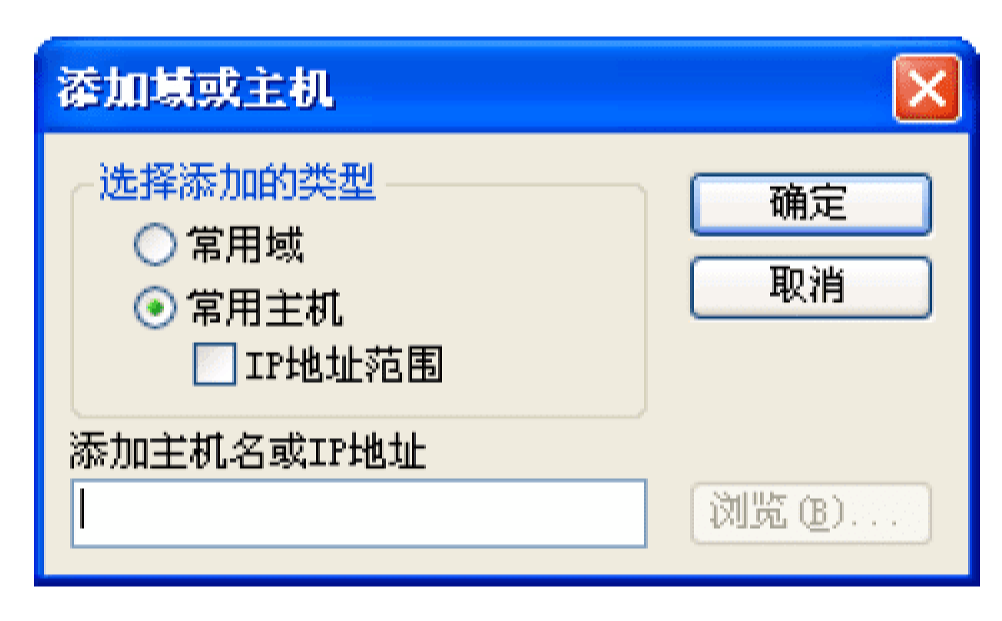



图 9-26 添加域或主机



图 9-27 添加主机和 IP 地址

（4）主机地址添加成功后如图 9-28 所示。

通过 DameWare 能够对 192.168.86.84 做如下操作：磁盘操作，事件日志，组管理，查看已打开文件，打印机，进程管理，系统属性，RAS，注册表，远程命令执行，远程控制，应用程序控制，计划任务管理，查找，发送信息，服务管理，会话管理，共享管理，远程关机，软件管理，系统工具，TCP 工具，用户管理，远程唤醒，如图 9-29 所示。

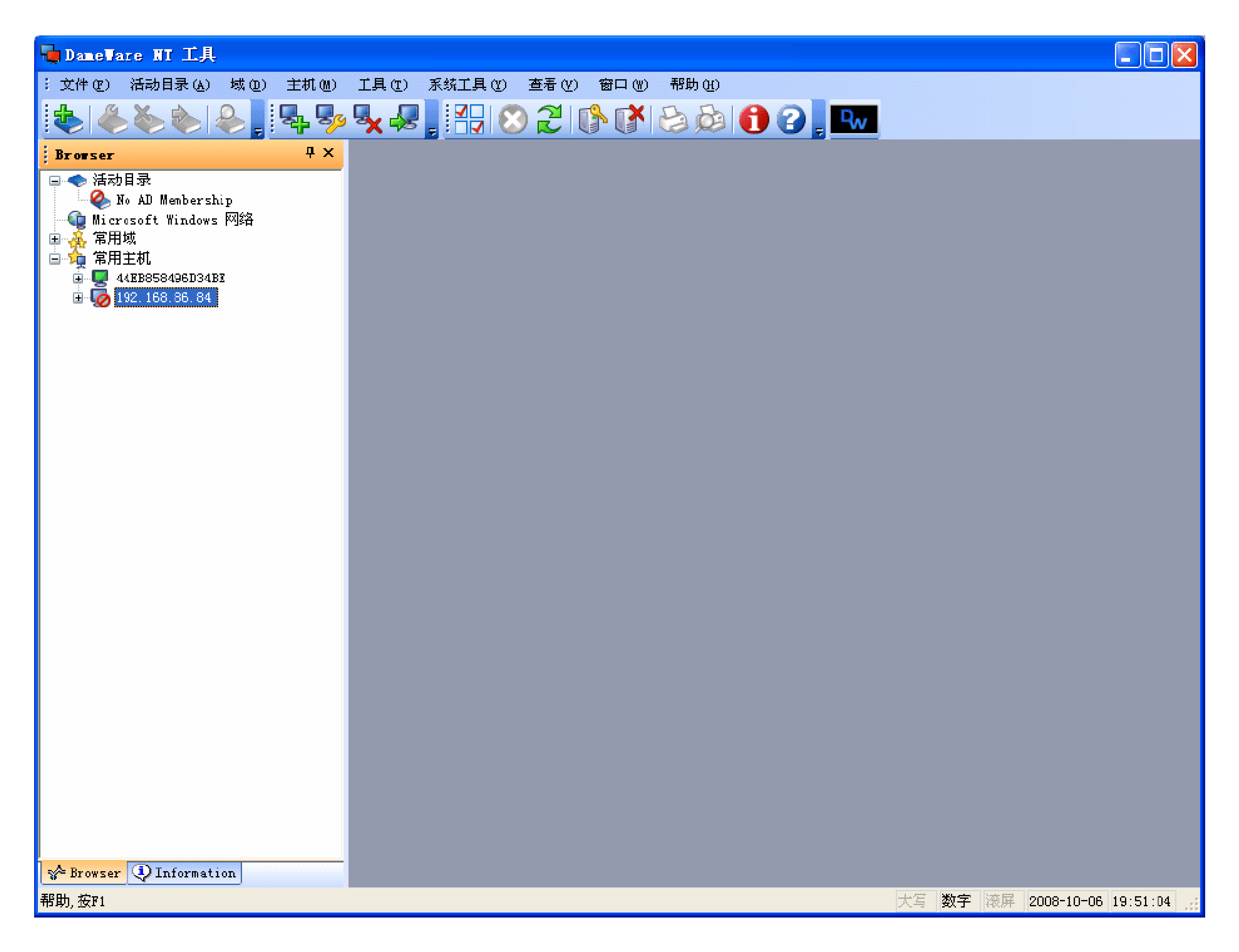


图 9-28 主机地址添加成功

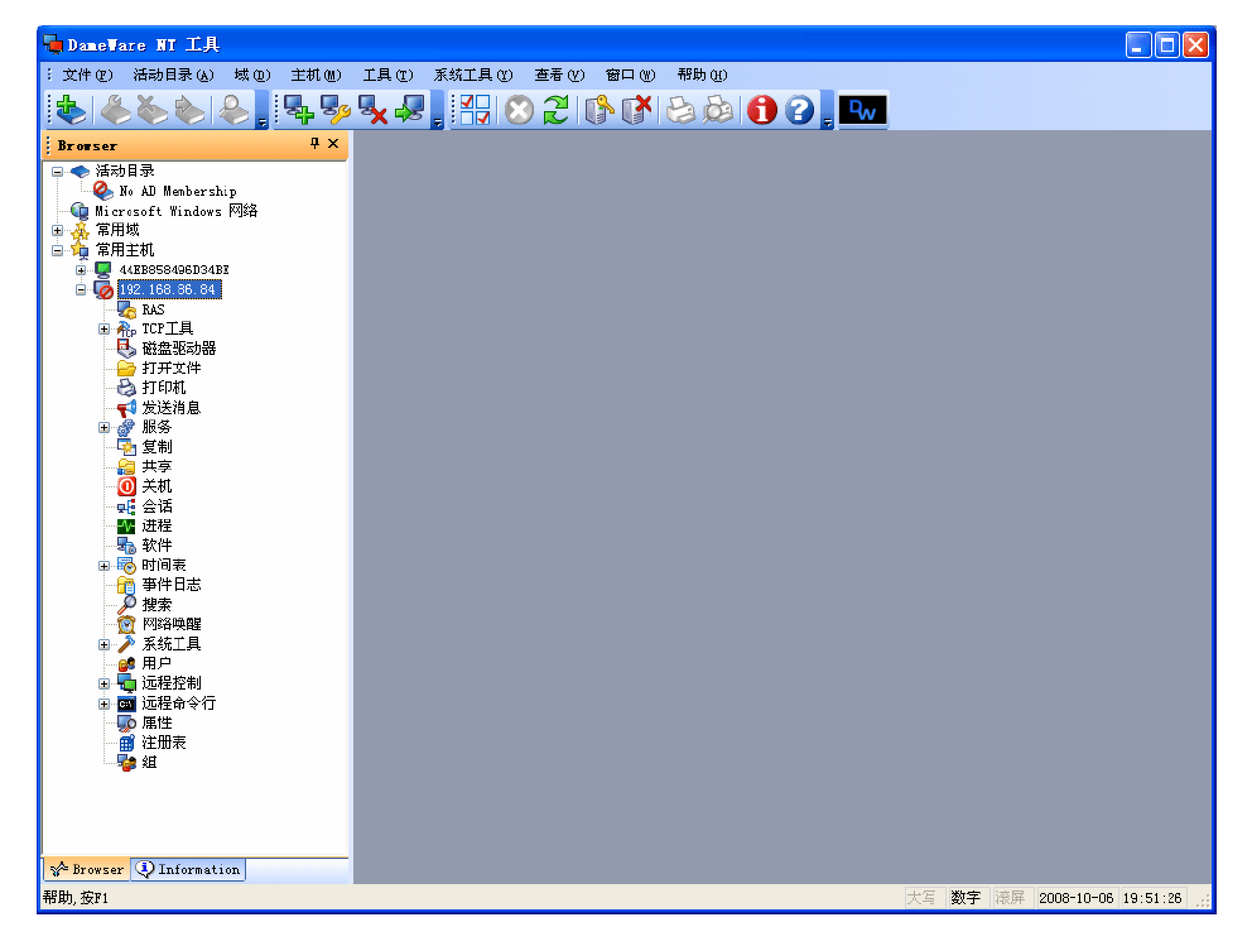


图 9-29 主机操作

还可以打开 Windows 自带的管理工具，如图 9-30 所示。

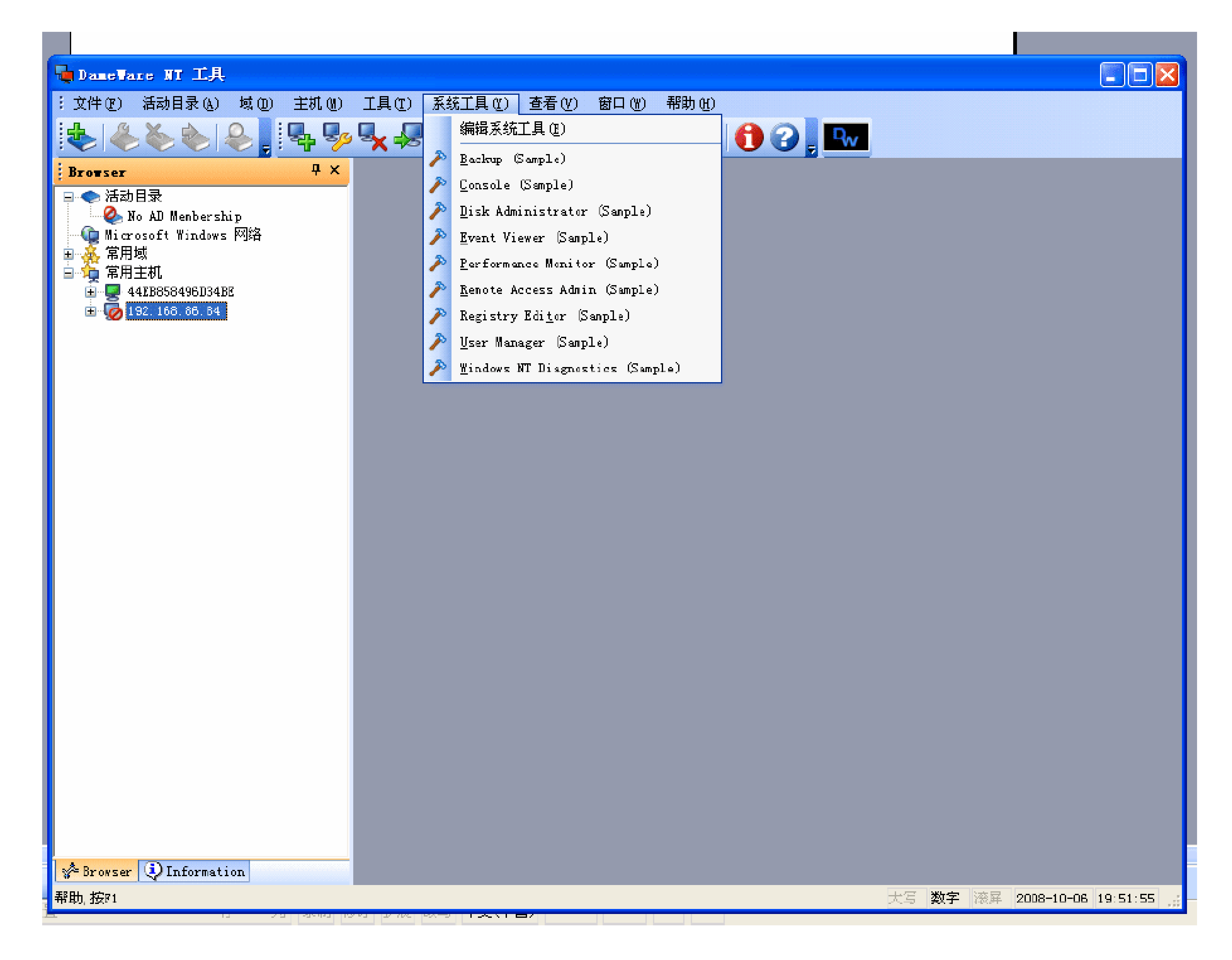


图 9-30 打开 Windows 自带的管理工具

3．实时屏幕监视和控制

在 DameWare 主界面中，单击远程控制图标进行远程控制，在打开菜单中双击迷你远程控制按钮，然后在弹出界面的“用户名”栏中填入获得的用户名“administrator”，“密码”栏不填，其他设置默认，填好后如图 9-31 所示。



图 9-31 远程连接设置

此时单击“连接”按钮进行连接，如果是首次连接远程主机，那么会要求为远程主

机安装 Dameware 被控端，如图 9-32 所示。

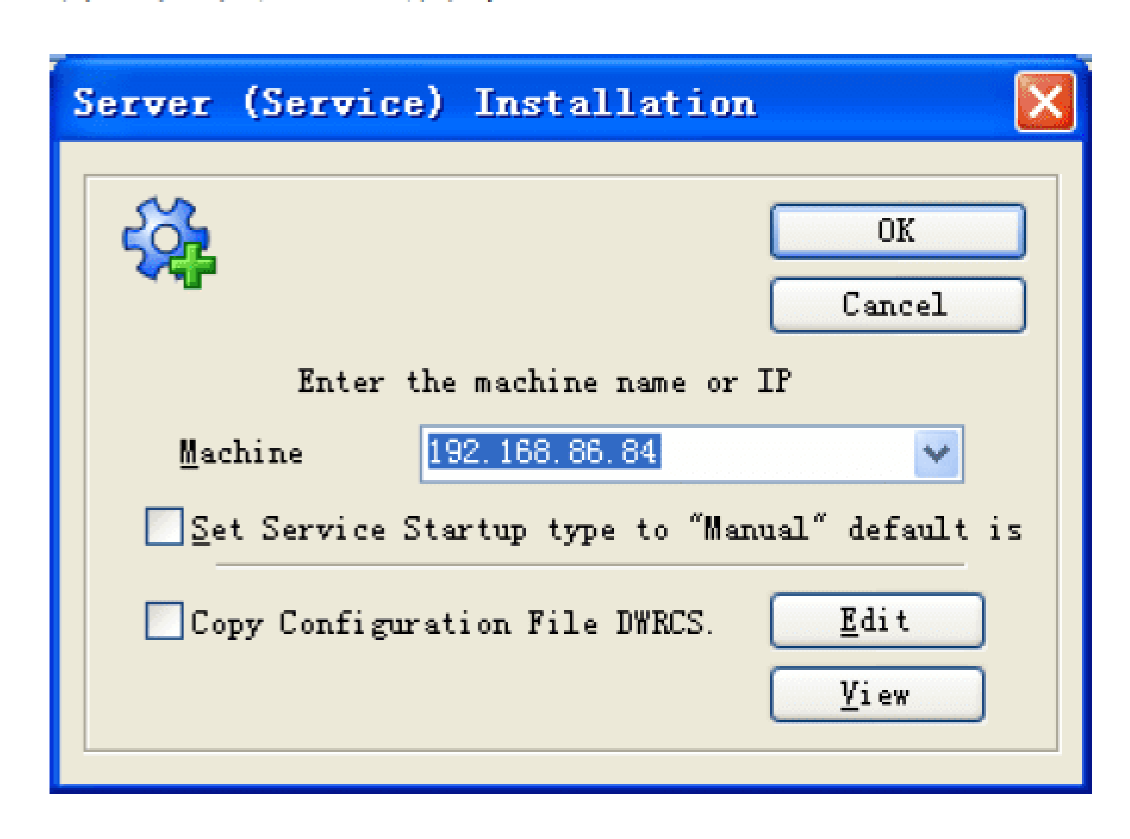


图 9-32　安装 Dameware 被控端

单击 OK 按钮，进行安装。服务安装、启动完毕后，便会在本地机上得到远程主机当前的屏幕，如图 9-33 所示。

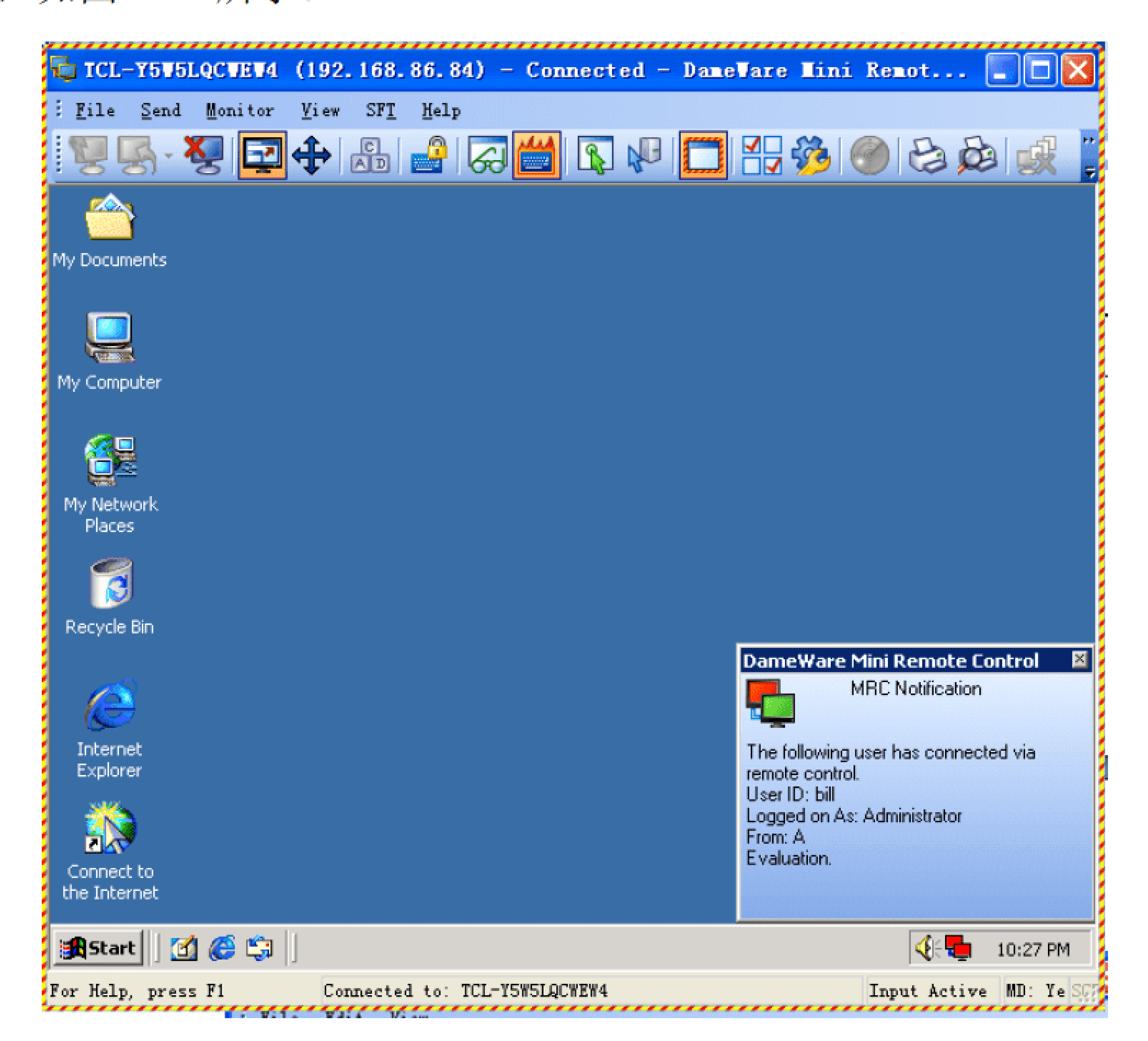


图 9-33　远程主机的当前屏幕

还可以通过该屏幕对远程主机进行控制，还可以在远程主机上进行键盘控制操作，甚至锁定远程主机上的键盘和鼠标。

4．远程执行命令

通过自带的工具 RCmd View 及 RCmd Console 来实现这一功能。DameWare 主界面中，单击列表中“远程命令行”前面的⊞找到查看 RCmd 和 RCmd 控制台来远程执行命令。通过这个工具，可以在远程主机上执行命令，如图 9-34 所示。

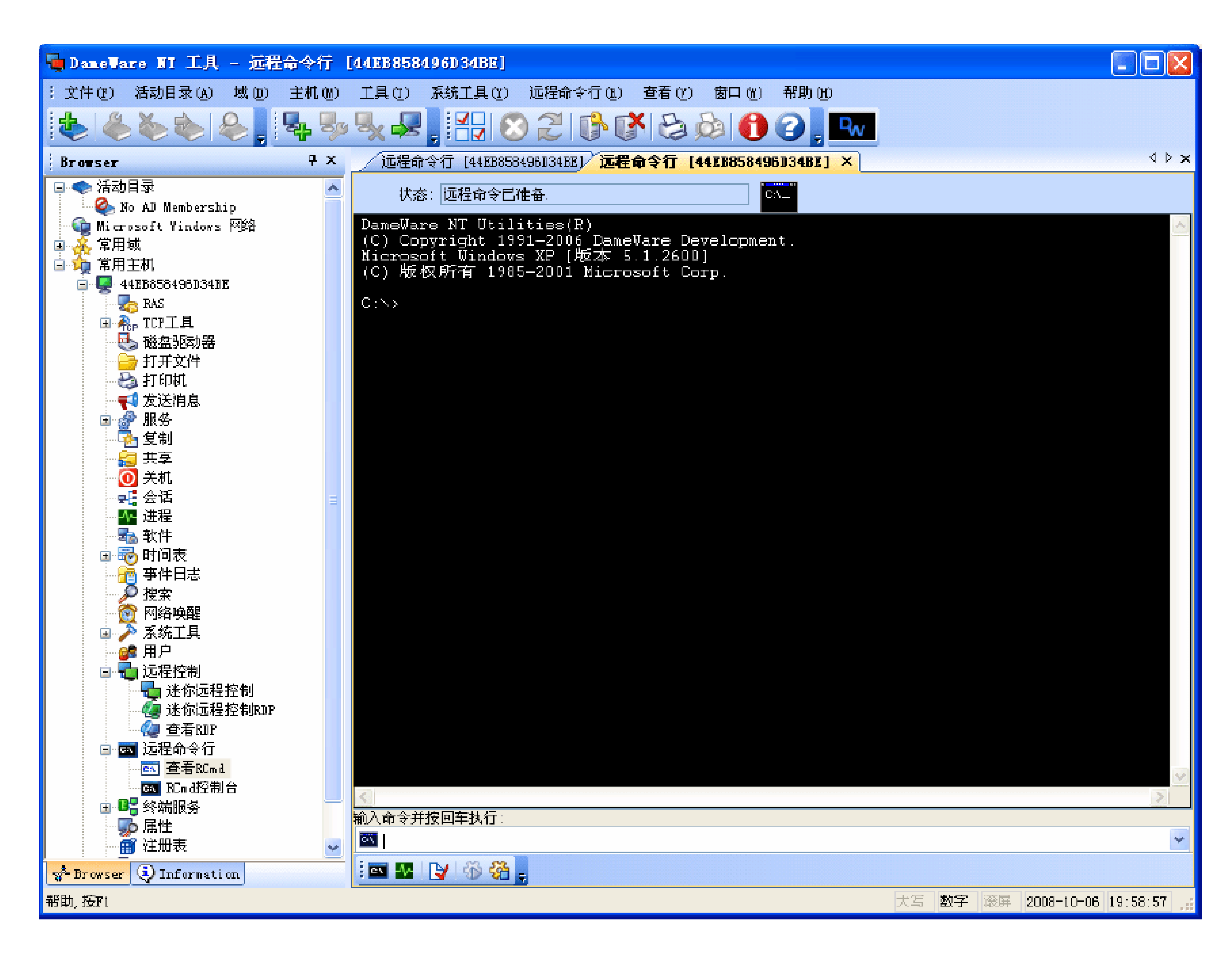


图 9-34　远程执行命令

5．修改系统参数并远程控制系统

（1）进程控制

选择 进程图标，打开后界面如图 9-35 所示。

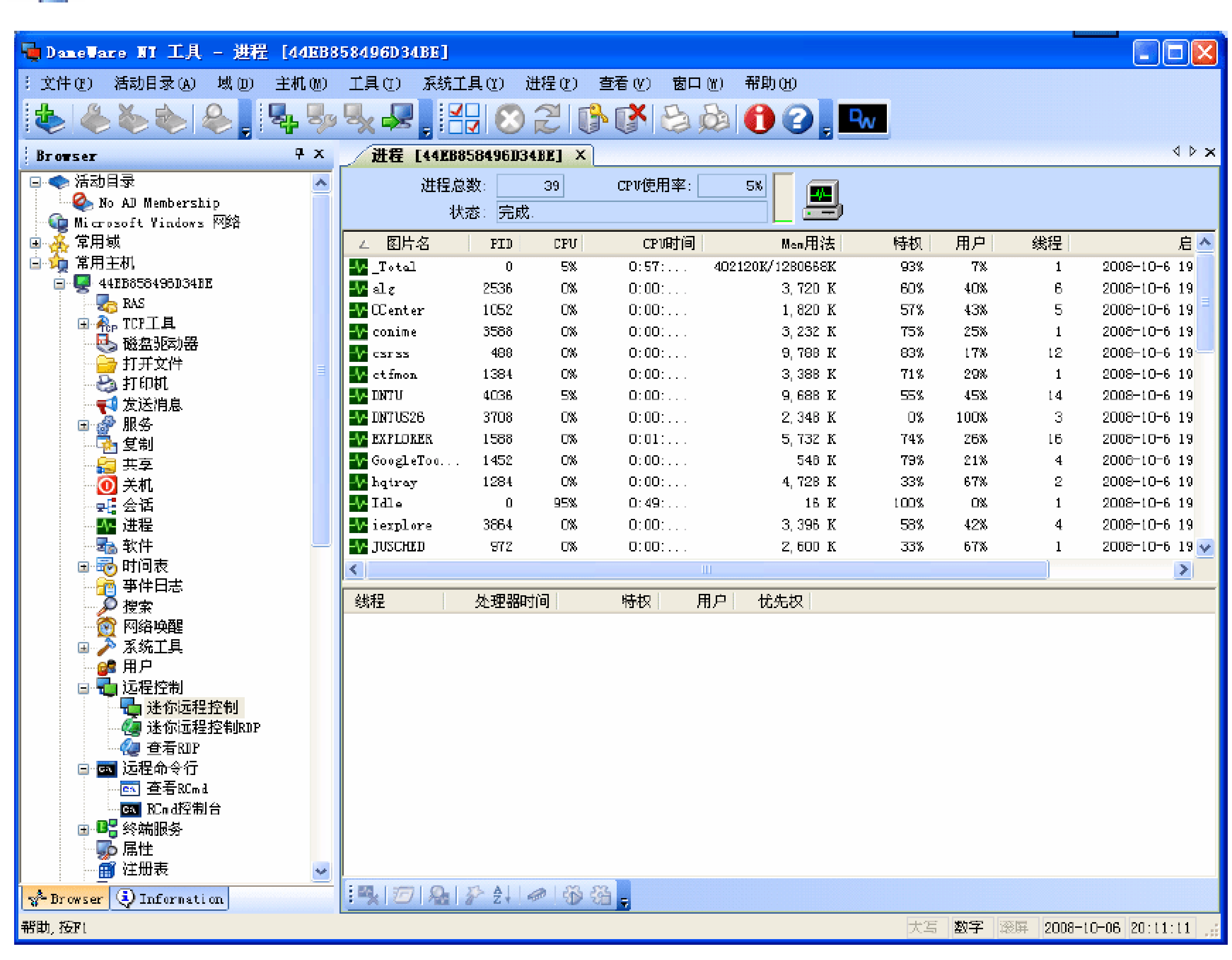


图 9-35　进程控制

右侧窗口显示的就是 192.168.86.44 的进程及 CPU 利用率。

（2）修改注册表

单击注册表项打开 192.168.86.44 上的注册表。在该注册表编辑器中便可以修改远程主机的注册表，如图 9-36 所示。

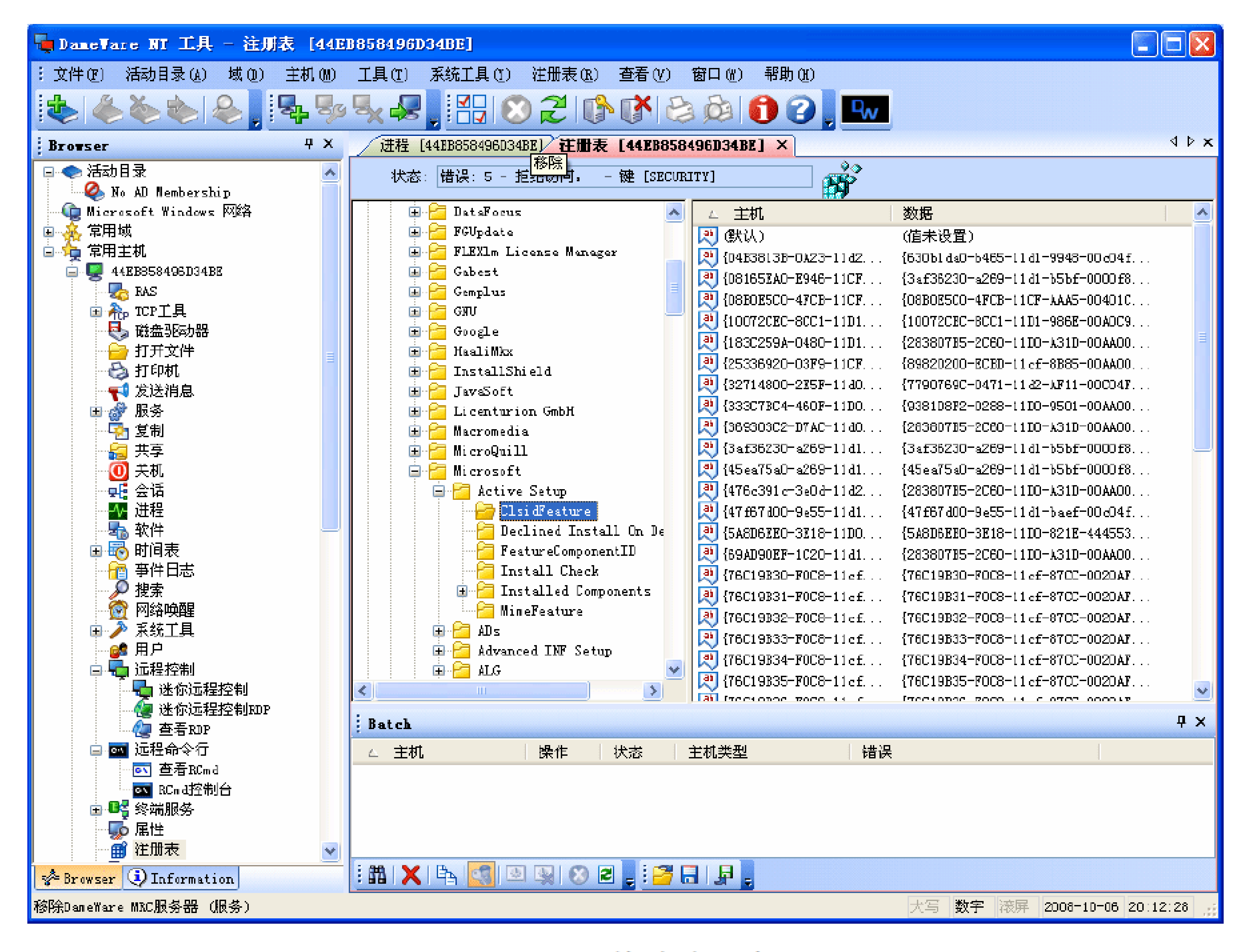


图 9-36　修改注册表

（3）建立计划任务

单击时间表项后得到如图 9-37 所示的树状菜单。

代表计划任务，双击后如图 9-38 所示。

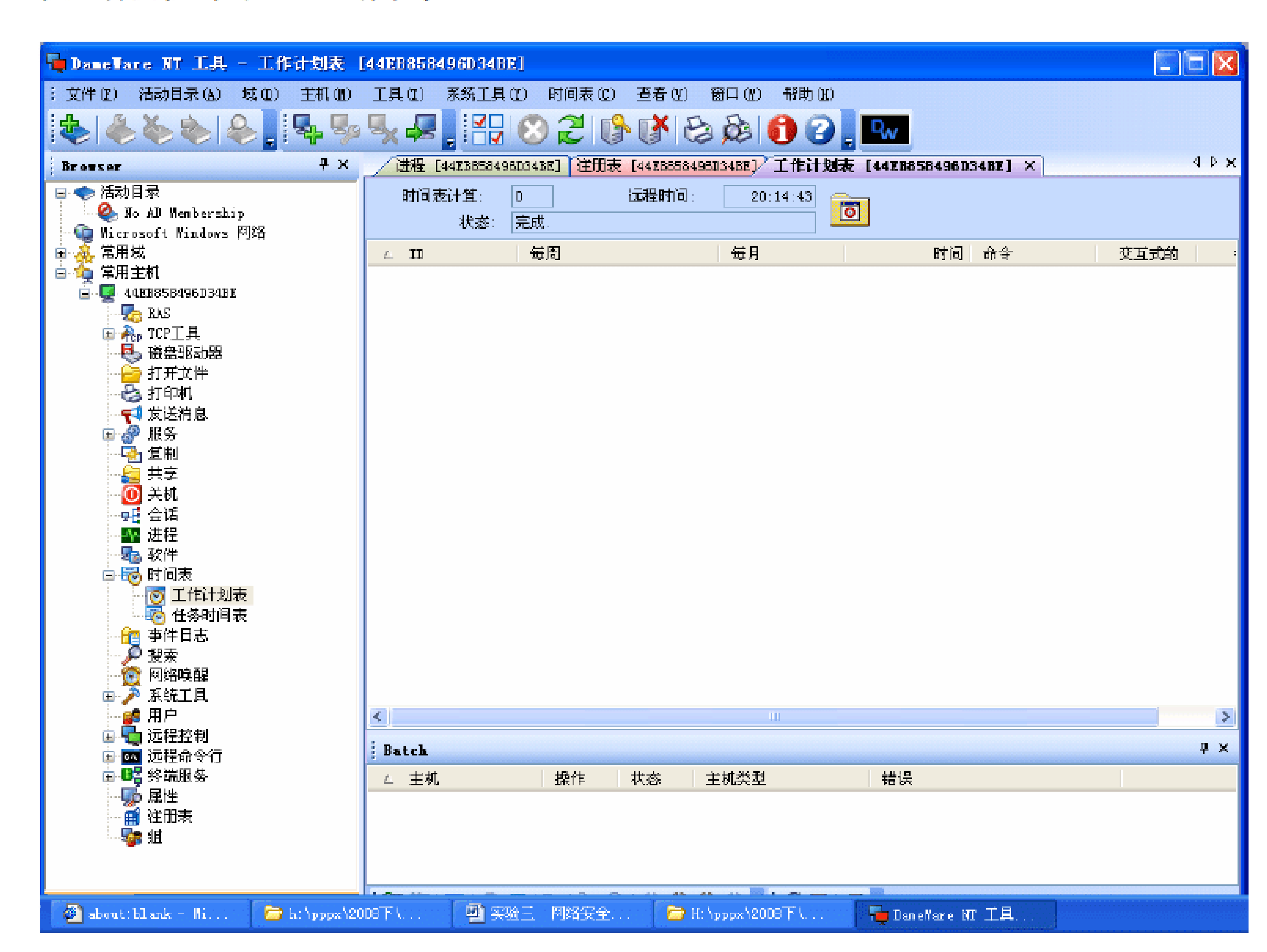




图 9-37　展开时间表

图 9-38　工作计划表

在主界面的“时间”下拉菜单中选择“添加时间表”命令即可实现建立计划任务，时间表属性设置如图 9-39 所示。

（4）服务管理

展开 服务得到如图 9-40 所示的树状菜单。

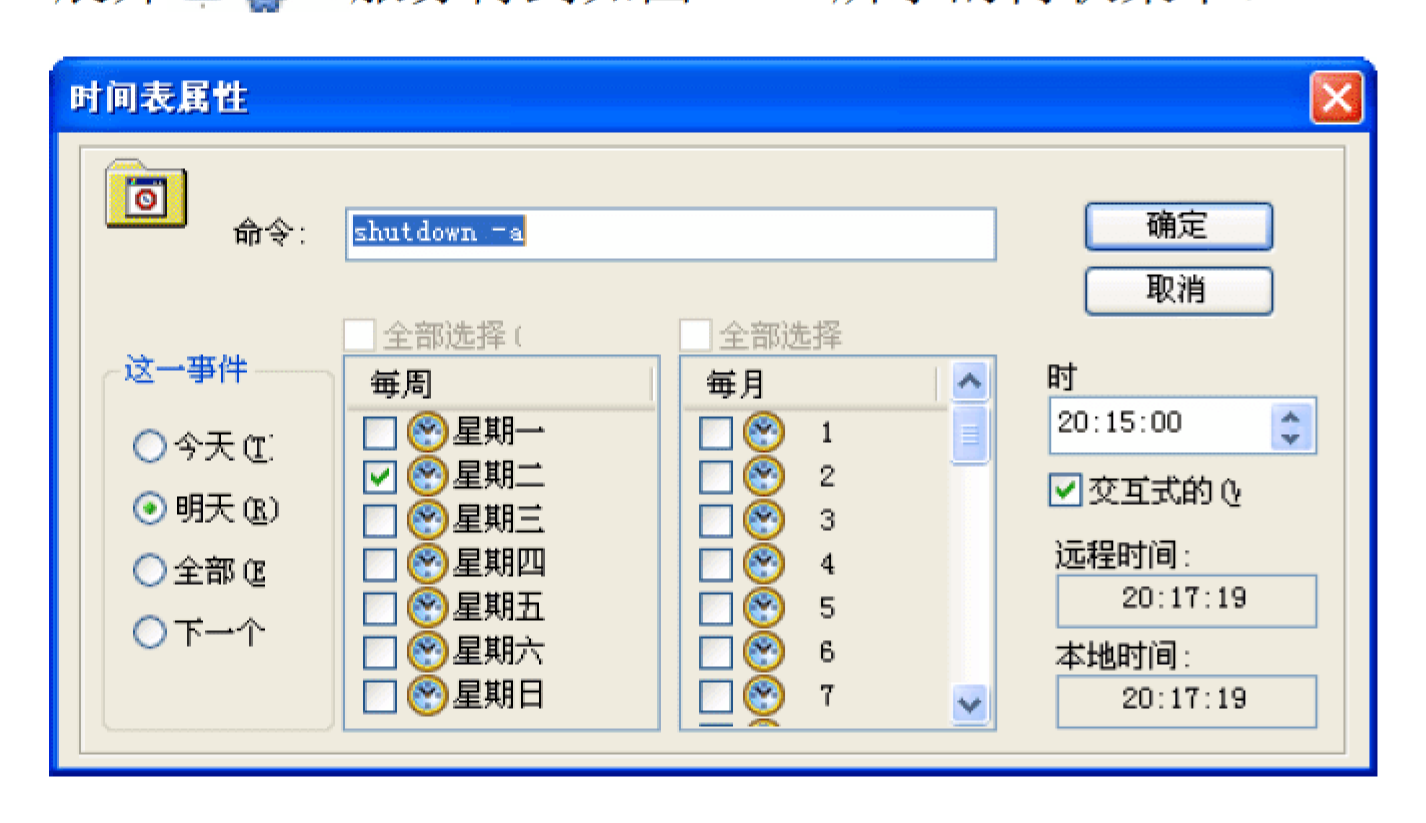


图 9-39　时间表属性



图 9-40　展开服务

通过 查看服务可以查看 192.168.86.44 上安装了哪些服务，如图 9-41 所示。

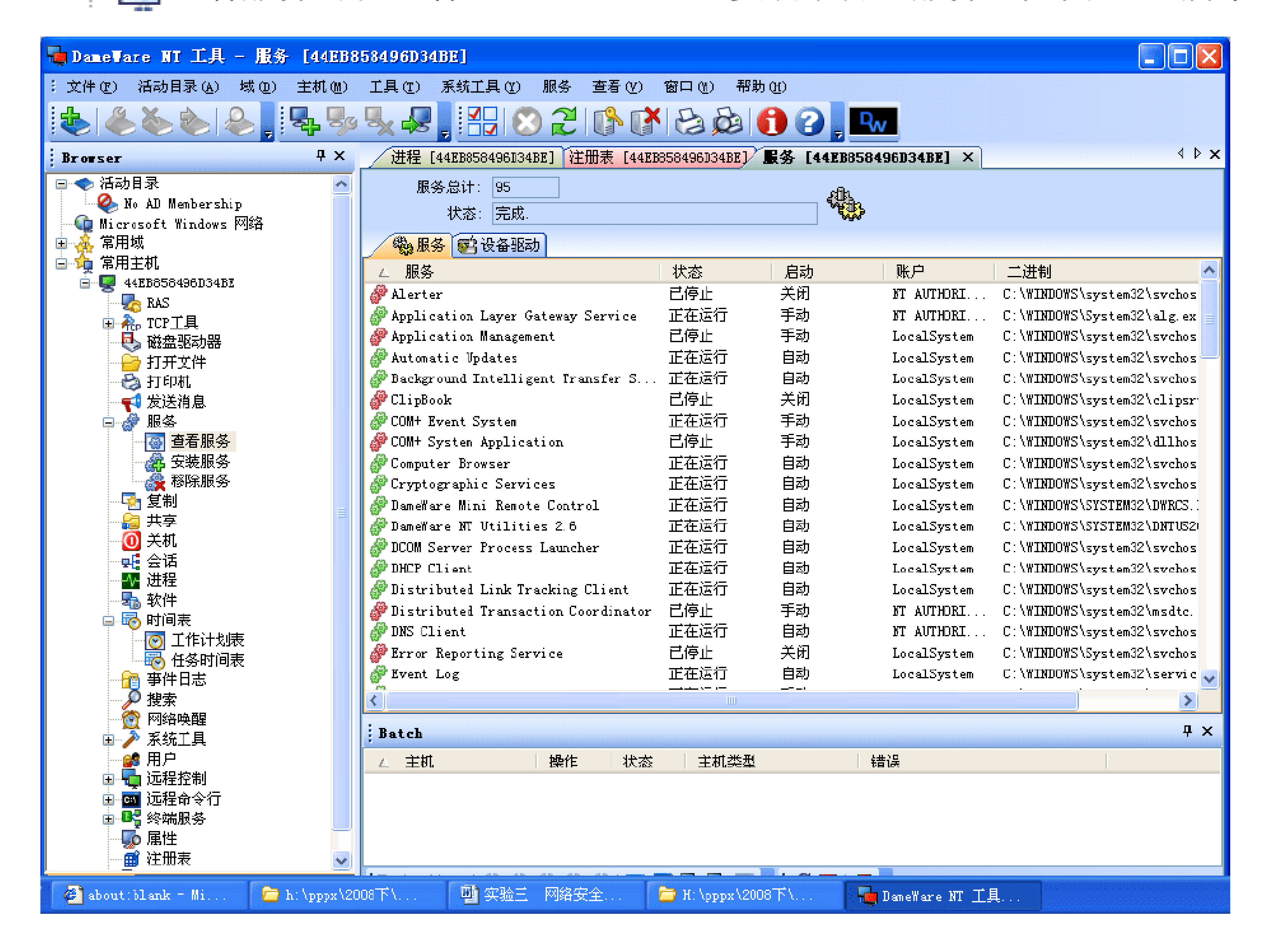


图 9-41　查看服务

（5）远程关机

单击 关机按钮可以实现远程关机，如图 9-42 所示。

（6）文件上传与下载

通过 共享来打开远程主机上的共享文件夹。可以对文件进行复制、剪切、删除、

隐藏、权限设置、粘贴等操作，如图 9-43 所示。

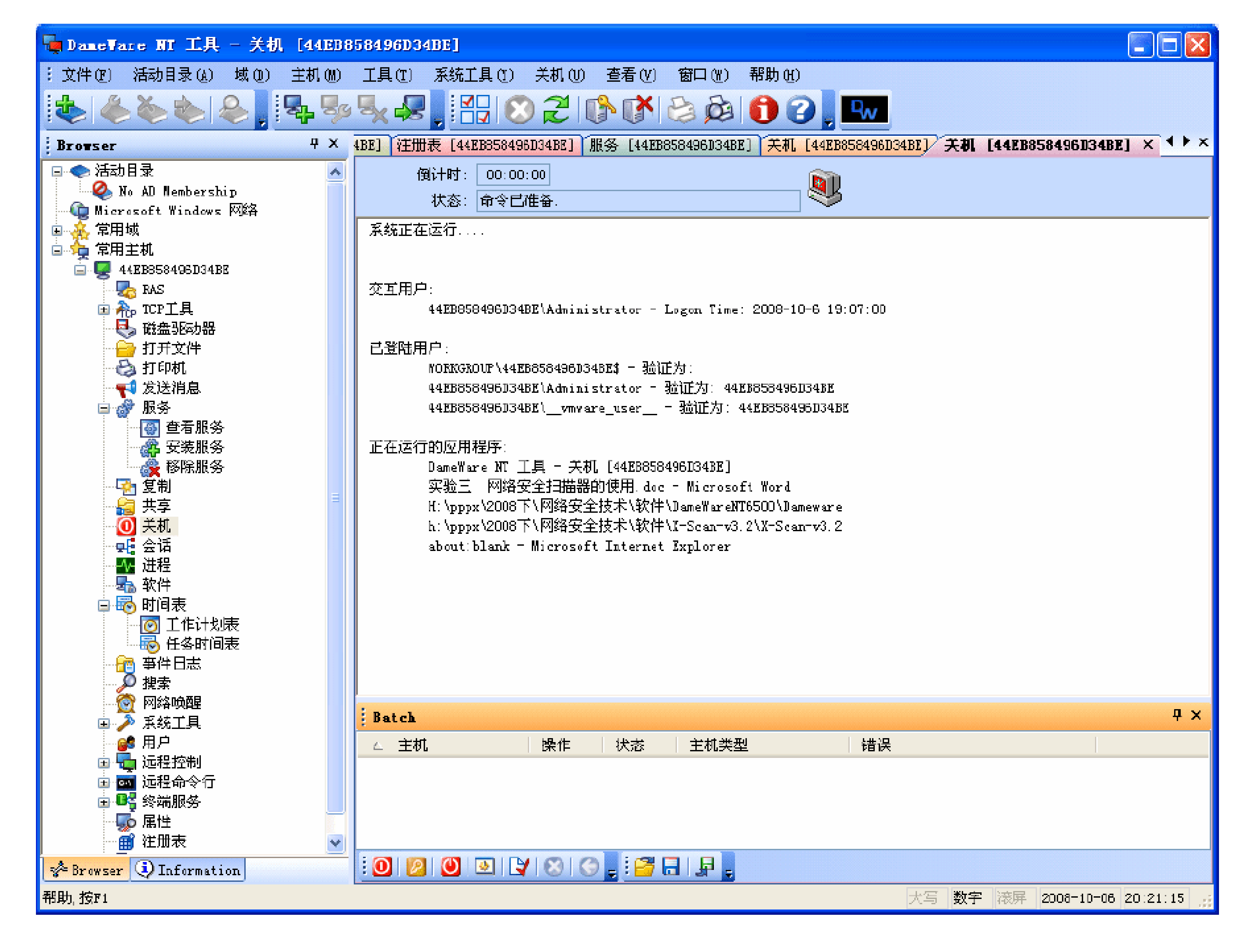


图 9-42　远程关机

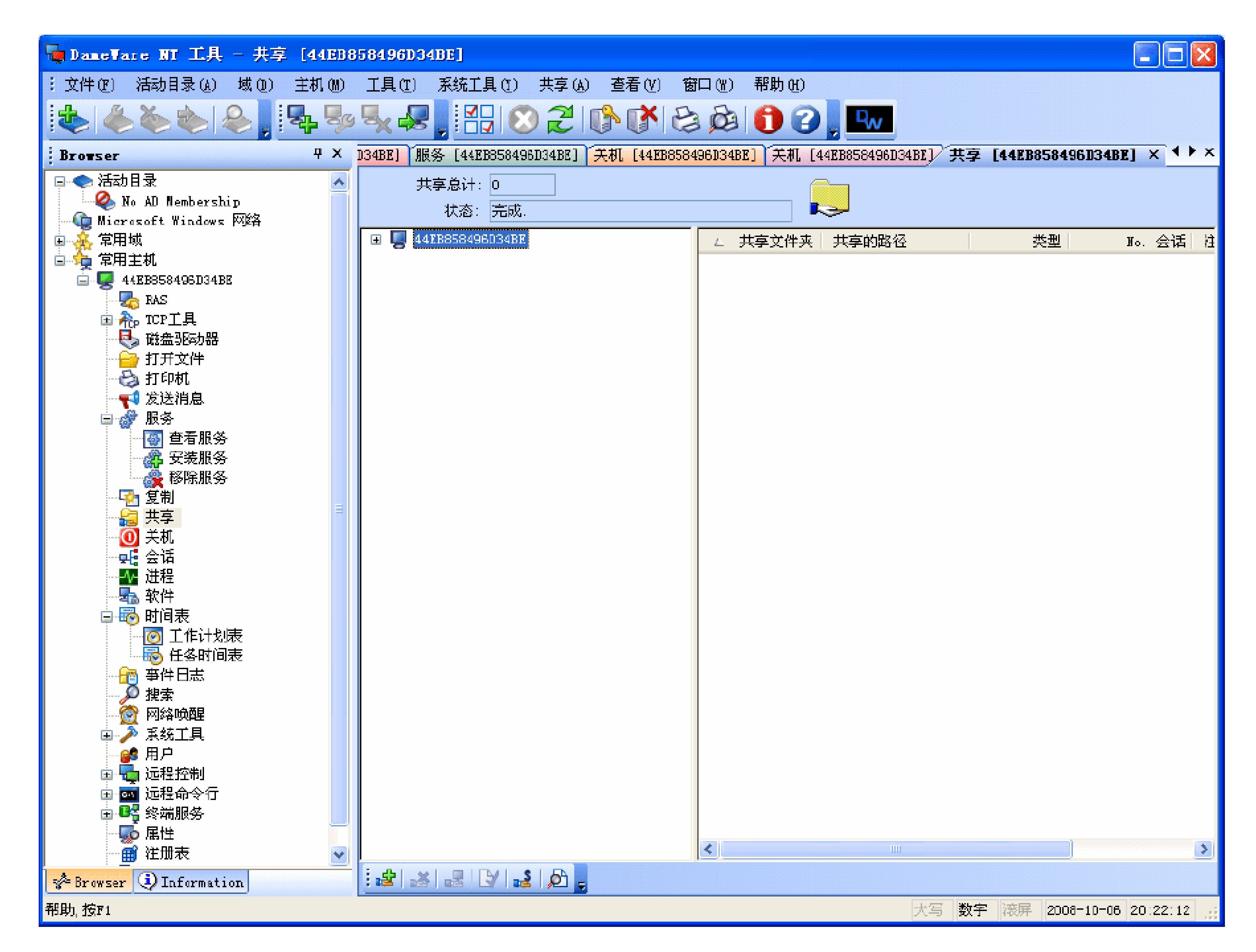


图 9-43　文件操作

（7）建立后门账号

单击 用户，打开用户管理，可以建立、禁用、降级、删除用户，如图 9-44 所示。

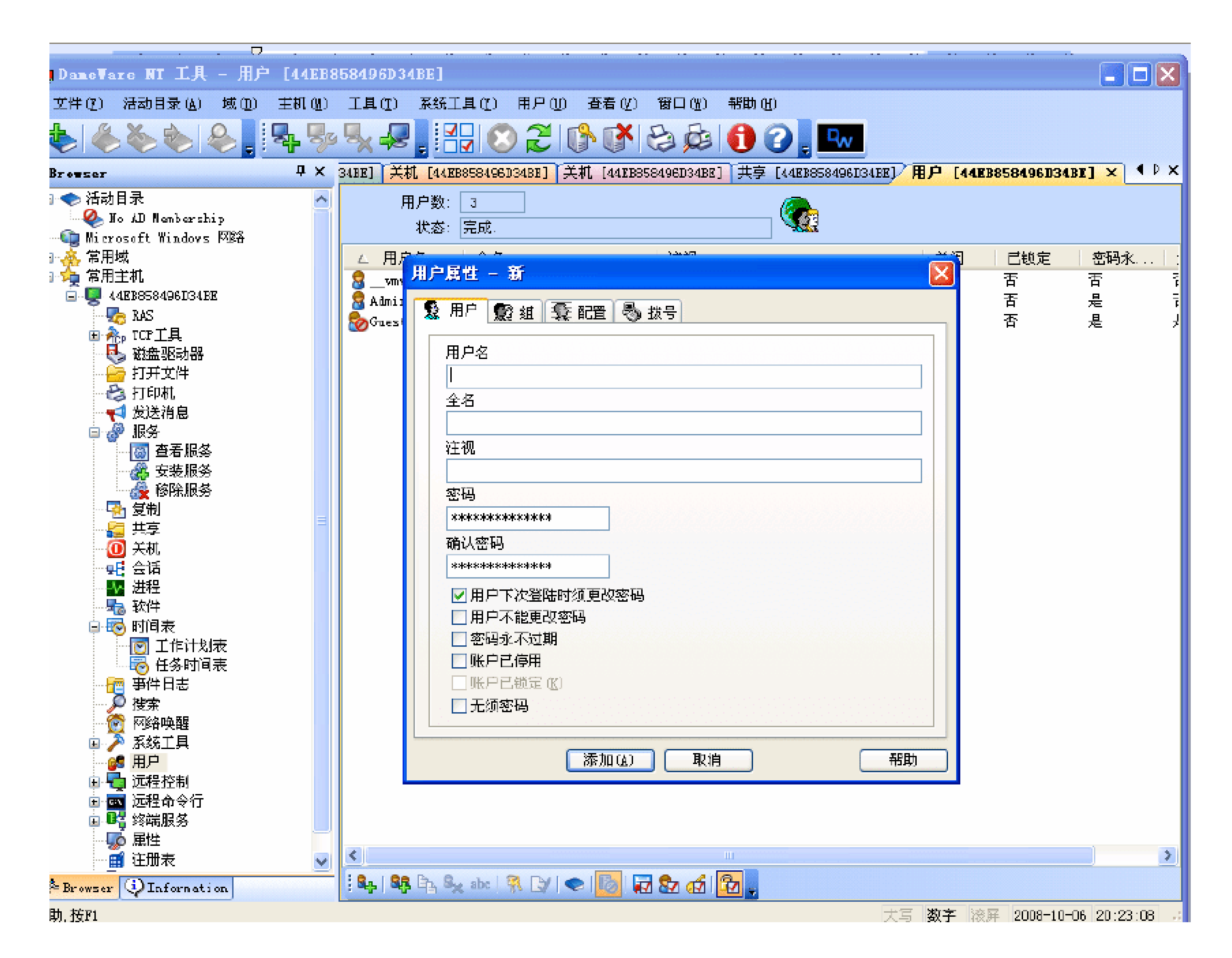


图 9-44　用户管理

（8）清除脚印

在离开 192.168.86.44 之前，需要清除脚印来防止管理员发现他们留下的痕迹，这可以通过删除日志来实现。单击 ![]事件日志，清除右侧窗口中的 Application、Security 和 System 日志。选择清除所有事件来清空 Application 日志。按同样的方法删除 Security 和 System 日志，如图 9-45 所示。

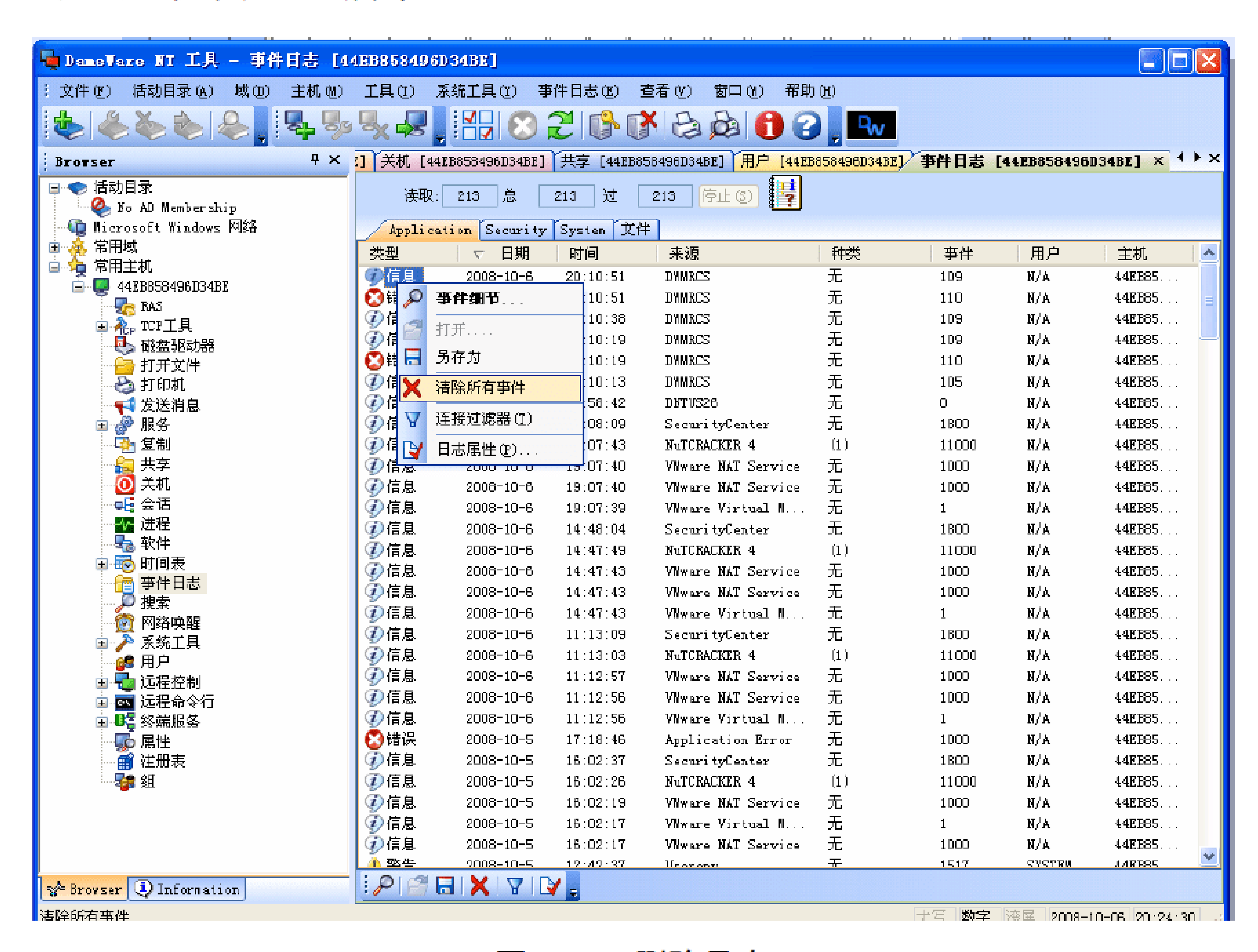


图 9-45　删除日志

第 10 章　病毒防范与过滤技术

本章学习重点：

- 内容过滤在计算机安全中的位置和重要性
- 病毒的原理及防范
- 垃圾邮件防范的有关技术

内容过滤是保护用户安全和数据安全最有效的手段。内容过滤是在通信内容进入用户网络或用户 PC 之前除去不必要的、有异议的和有害内容的过程。内容过滤可以设置在网络的多个位置上，包括用户 PC 上、组织内部服务器上等。内容过滤可以由 ISP（互联网服务提供商）或第三方网站实现。

10.1　内容过滤技术

随着互联网技术的发展，尤其是万维网应用的不断增加，人们可以从网络上获得任何想要的资源，这给人们的工作、生活、学习带来了巨大的便利和好处。但与此同时，网络资源也成为攻击者实施攻击的主要手段，他们利用网络技术中存在的漏洞，将病毒、木马以及其他具有恶意企图的代码或程序隐藏在网页或下载的资源中，以此达到入侵用户系统，进行任意破坏的目的。过滤就是根据系统事先设定的规则（例如 IP 地址）对用户从网络上获取的资源或网页内容进行检测，防止恶意代码或程序到达用户电脑，达到保护用户系统安全的目的。

10.1.1　过滤的种类

1．白名单过滤

白名单过滤是根据白名单列表进行的。这个白名单列表是一个允许访问列表，由第三方审查和编译。列表上的所有内容都是允许访问的，可以是一个允许访问的网页的 URL 列表，一个合法关键词列表，或是一个合法通信数据包的包签名列表。

白名单方法在内容过滤上起到了很好的效果，但也存在一些缺点，具体如下。

（1）难以建立一套适于全球范围的标准。由于 Internet 是一个涉及多种文化、宗教以及政治的综合体，建立一套被全球接受的指导方针几乎是不可能的。

（2）规模难以控制。随着接收条目的日益扩大，白名单规模越来越大，有可能超出控制。

（3）缺少管理名单的中心权威机构。事实上，这是使用白名单方法进行内容过滤的最大的一个困难。例如，尽管多年来用户们一直受到病毒的困扰，可是并没有一个由中心权威机构发布的包含了所有已经被制造出来的病毒签名的名单。

2. 黑名单过滤

内容过滤的另一种方法是使用黑名单过滤。这种方法与白名单过滤正好相反。黑名单过滤是基于有害内容的名单进行的。这个名单可能包含网站的 URL、关键词以及通信数据包的签名等内容。由于黑名单规模的有限性以及易管理性，这种方法比白名单过滤更常见。

黑名单过滤存在的问题是黑名单不能及时更新，是不完整的。事实上，在计算机病毒领域同样存在这些缺点。还不存在一份包含全部已知病毒签名的名单，反病毒公司正在不断地升级更新病毒名单。

3. 内容过滤实现原理

黑白名单过滤都依赖于一张已知的列表。这张列表组成元素网页 URL、关键词、短语、数据包签名、属性、图像分析等内容。下面介绍基于这些要素的内容过滤的原理。

（1）URL 过滤

这种方法是根据流入或流出网络的网页内容的 URL 进行过滤的。这是内容过滤最常见的一种方法，尤其在阻止访问某些特定网站的时候使用最多。URL 过滤只是根据非法网站的 URL 地址进行过滤，因此并不影响网站所在主机的 IP 地址，因此网页所在主机依然能够为网络或 PC 提供其他服务。

为提高准确性，URL 过滤在目标的模式设置上要注重很多细节。另外，由于底层细节的需要，更改 URL 文件的时候也必须同时更改过滤器中的相应设置。

（2）关键词过滤

关键词过滤需要鉴别所有流入流出内容的关键词，根据所使用的扫描机制，语法上正确的词语还需要进一步和白名单或黑名单上的词语比较。这种方法包含了以下这些缺点。

- 基于文本的特性使这种方法不能对其他形式的数据进行检查。
- 基于语法的特性使得这种方法忽略上下文的语义环境，容易在造成误报。

（3）包过滤

这种方法根据网络通信数据包的 IP 地址对内容进行过滤。也就是说如果某一台机器的 IP 地址存在于阻塞规则中，那么任何来自或去往这台机器的通信内容都会被阻塞。由于是根据一台计算机的地址而不是根据其通信内容进行阻塞，意味着这台计算机提供的其他正常服务也被同时阻止了。当然，包过滤还可以根据数据包的端口号、序列号等其他内容来进行。

（4）属性过滤

在内容过滤中使用人工智能是内容过滤器的一个新分支，此种方法根据当前的文本特性进行学习，以达到区别未知文本的目的。然而，由于过程的复杂性以及耗时性，这种方法目前还没有被广泛使用。在预处理过程中，需要取回一部分文件并对其进行学习，此过程可以是基于文本的也可以是基于内容的。

（5）图像分析过滤技术

自从带有多媒体内容的万维网首次出现，其他不同于文本形式的 Internet 通信开始

增加，尤其是音频和视频的内容日益增加。为兼容这些形式，并能够对这些内容进行过滤，必须找到新的方法。在所有这些方法中，有一种是根据图像分析进行的。这种方法存在着许多问题，包括图像的预下载问题、带宽问题、语法过滤导致的语义难区分性等。

10.1.2 内容过滤的位置

放置内容过滤最好的 4 个位置是：用户 PC 上（最重要的位置），互联网服务提供商 ISP 的网关上，组织服务器上，以及第三方的机器上。

1. 用户 PC 上的过滤

用户 PC 是设置内容过滤最重要的位置。使用安装在用户 PC 上的软件，用户能够设置阻塞规则以及阻塞列表，阻止进入的通信内容。在这种情况下，用户就变成实施内容过滤的关键。同时还负责更新阻塞规则和阻塞列表，提供保措施护和阻塞列表使内容免于被非授权修改。

2. ISP 计算机上的过滤

ISP 上的过滤和用户 PC 上的过滤不同，是由 ISP 设置和管理过滤规则和过滤列表的。同时，这种方法增加了过滤规则和过滤列表免于未授权更改的安全性。当然，这种方法也减弱了用户需要的表达。

因为这种方法是集中过滤，有着很多其他方法没有的优点：第一，ISP 拥有更多的可用资源，能提供更多的安全；第二，ISP 能够使用完整的机器——代理服务器来执行过滤，使得过滤的过程更快；最后，ISP 拥有比个人用户更加详细的过滤列表和数据库。

安装代理服务器之后，进入或离开 ISP 的通信必须通过代理服务器才能访问 Internet。可以安装代理服务器来阻塞一定的服务。

3. 组织内部服务器的过滤

为了满足组织的需求，可以在组织内部特定的服务器上实施内容过滤。就像在 ISP 上实施过滤一样，组织的系统管理员能够选取特定服务器来过滤进入或离开组织的内容，所有进入或离开系统的通信必须通过这个过滤器。这也是一种集中过滤方法，过滤规则和过滤列表都是被中心控制的，具有极高的安全性。

4. 第三方过滤

对于不能进行自主过滤的组织和个人，第三方内容过滤是一种不错的安全选择。进入和离开用户或组织网关的通信内容被导流通过第三方的过滤器。第三方组织可能像 ISP 一样使用代理网关，或者像组织服务器一样选择特定的服务器。第三方过滤器提供了更高的安全度以及更多样的过滤选择。

5. 典型案例——防病毒过滤网关的应用

近年来，企业用户特别容易遭受到病毒的侵袭，病毒正在通过更多的传播方式进入

企业内部。有数据显示，目前 90%的病毒是通过邮件传输进入企业内部的，而不是通过以前的存储介质进行传播，此外浏览网页、FTP 下载等都成为病毒传播的手段。而企业采用的防病毒解决方案主要是基于单机或服务器的方式，是一种被动的解决方案。每当出现新的病毒，企业安全部门往往会发现他们分身乏术，需要确保网络中的每一台电脑、笔记本、PC 和服务器等都升级到了最新的病毒库。传统的病毒处理方法会存在一些问题，具体如下。

（1）扫描和处理方式主要是通过客户端杀毒，或者通过企业版防毒软件对已经进入企业网络的病毒进行处理，是一种被动的杀毒模式。

（2）越来越多新的蠕虫病毒传播速度很快，传播范围很广，充分利用企业网络的开放性，在企业没有防备的时候迅速进入企业内部并很快在网络中传播开来，造成企业网络阻塞等情况。

（3）越来越多的像网络钓鱼这样的网络欺诈行为通过网络应用协议骚扰和破坏企业的正常办公网络环境。

为了解决上述日益严重的问题，防病毒厂商提出在企业的网关处对进出企业的主要网络协议的数据进行病毒过滤扫描，这样就可以把病毒阻挡在企业外部，大大减少病毒进入企业内部造成的危害。因此防病毒网关产品应运而生，同时防病毒网关产品也成了企业防病毒解决方案中不可缺少的一部分。

随着网络应用的发展，企业用户对网络处理性能的要求越来越高，基于硬件的信息安全专用产品可以很好地满足用户需求。对于硬件防病毒过滤网关来讲，其便捷性更为突出。厂商在产品设计上采用安全精简的定制操作系统，基于专用硬件平台等办法，保证数据在网络中的能够快速处理。软硬件一体的防病毒过滤网关已经成为企业整体防病毒解决方案中重要的组成部分，它配合桌面防毒软件和企业版的防毒软件，在企业的入口处最先拦截企图进入网络的病毒，给后面的客户端防毒减少了很大的压力。全球安全业界普遍认为防毒墙将成为企业级防毒市场的主角，行业前景非常可观。ICSA 认为，硬件防毒墙将占据整个防病毒产业的一半市场份额，成为防病毒行业标准。

目前，各大厂商都推出了自己独特的软硬件一体防病毒过滤网关。这些产品一般都具备如下优点。

（1）采用高效的流扫描算法

防病毒过滤网关采用特有的流扫描技术来获得很高的吞吐率，同时大大减少网络延迟和超时。流扫描技术在收到文件的一部分时就开始扫描，大大减少总的处理时间。

（2）真正的即插即用设备

防病毒过滤网关实现了真正的即插即用，不需要变动当前已经部署的网络。一旦部署的位置被确定，只需要连接上网线，开启电源就可以进行病毒扫描。

（3）支持双通道的病毒扫描和过滤

在过滤网关内部建立两条相互隔离的病毒扫描通道，在组网时，用户可以利用同一台过滤网关的第二条扫描通道单独对防火墙的 DMZ 区的服务器组实现病毒防护，更加增强了安全性，同时节省了企业的成本。

（4）全面应用网络协议

能处理所有主要网络协议——SMTP、POP3、HTTP、HTTPS、FTP 和 IMAP；同时

还增加了对协议非标准端口的病毒扫描。

（5）增加了 HTTPS 协议的病毒扫描

能对 https 的流量进行扫描，这样的功能大大增强了 B2B、B2C、C2C 等 https 网上交易的安全性。

（6）扫描方式透明

大多数传统的解决方案工作在 OSI 的应用层，以代理的方式截获数据进行扫描，客户机首先连接到防病毒网关，防病毒网关再连接到真正的服务器，转发并扫描通过的数据流，这种方法丢失了很多有用的客户端及服务器的信息。防病毒过滤网关工作在 3～7 层（图 10-1），它能够完整地保留这些信息，使企业的网络更安全。

OSI 网络层次	覆盖面	
7. 应用层	传统的防病毒软件	典型的软硬件一体过滤网关产品
6. 表示层		
5. 会话层		
4. 传输层		
3. 网络层		
2. 数据链路层		
1. 物理层		

图 10-1　防病毒过滤网关工作在 3～7 层

下面就是一个典型的企业防病毒过滤网关部署方案（图 10-2）：将过滤网关部署在防火墙和中心交换机之间。企业的网关处是防病毒过滤网关最合理和最有效的部署位置，网络病毒就是从那里进入公司内部网络。将过滤网关部署在网关处，可以在病毒进入网络的源头对它进行扫描和查杀。

10.1.3　内容过滤的层次

内容过滤可以在发生在两个层次：应用层和网络层。应用层的过滤是根据网页 URL 进行的，可以阻塞特定的网页或 FTP 站点。网络层的过滤是包过滤，要求路由器检查流入或流出的每一个通信数据包的 IP 地址（有些时候还包括端口号等其他信息），将其和白名单或黑名单上的数据进行对比。

1．应用层过滤

应用层过滤根据组成阻塞标准的类别进行，包括 URL、关键词等。应用层过滤同样能够被设置在很多的地点，包括用户 PC 上，网络网关上，第三方服务器上，以及 ISP 机器上。在每一个地点，每一个相当高效的过滤机制都能够被成功应用。当在网络上或在 ISP 上进行应用层过滤的时候，可能就会用到一个特定的代理服务器。代理服务器根据过滤规则阻止进入或流出服务器的内容。对于来自于用户或客户端的每一个请求，代理服务器将会把客户的请求以及包含有 Web 站点、FTP 站点和新闻组的黑名单进行比较。

如果用户请求访问的 URL 就在黑名单之上，代理服务器就会做出有效的阻塞手段。除了阻塞流入或流出网络或用户计算机的数据流，代理服务器还能存储经常访问的数据。然而，利用代理服务器进行的应用层阻塞的效率是有限的，主要因为下列这些技术上和非技术上的因素。

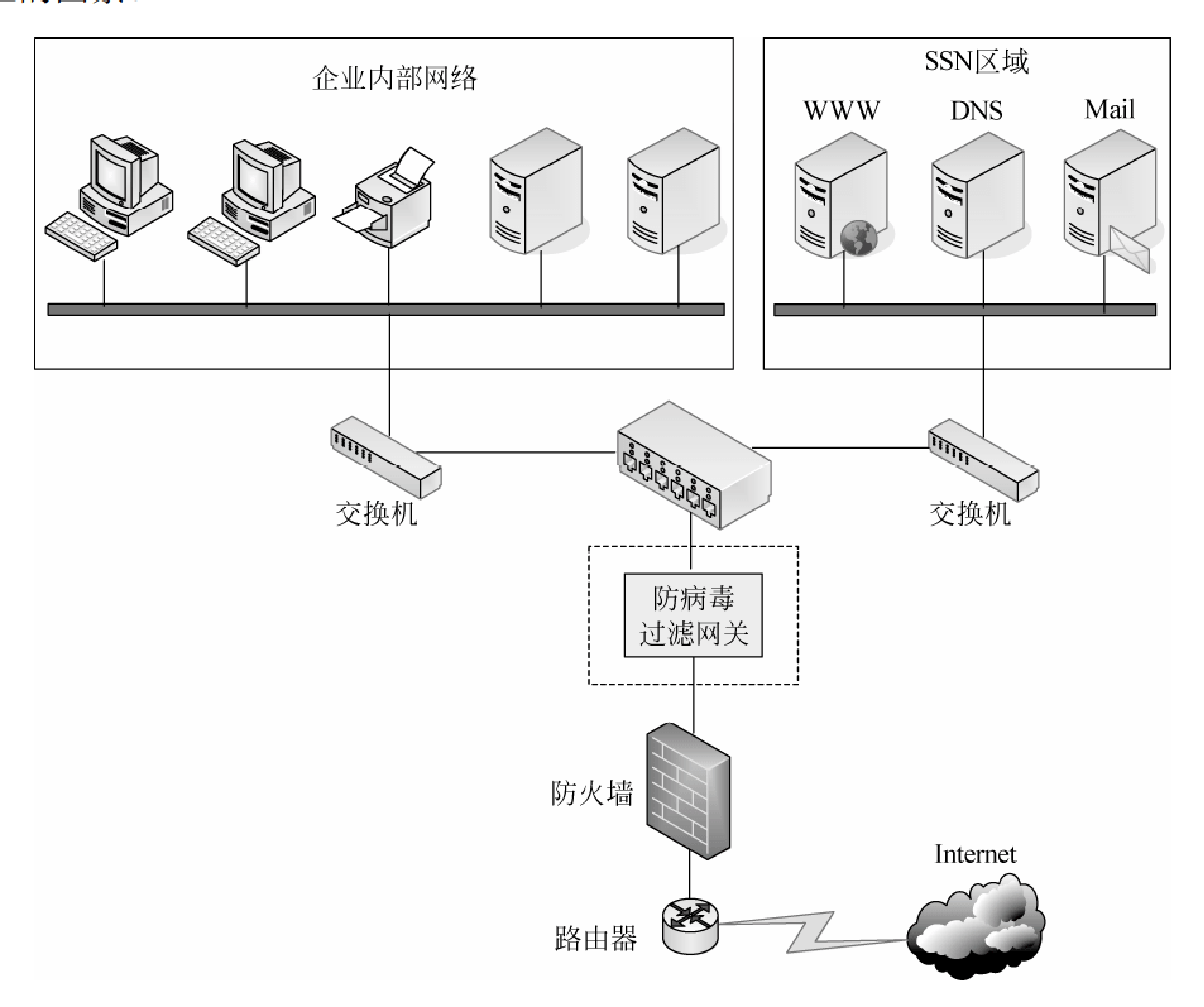


图 10-2　防病毒过滤网关部署方案

（1）技术问题

① 在用户请求中使用翻译服务能够造成来自于有害服务器和站点的请求内容进入网络：当用户请求来自于特定服务器或站点内容的时候，如果在这个站点上不能找到请求的内容，翻译服务就会向二次网站发起请求。在这种情况下，返回的内容就有可能不是来自于特定的服务器，除非二级请求已经被阻塞了。

② 绕过域名服务器：由于可以根据域名，也可以根据服务器的 IP 地址来处理用户请求访问的站点，因此，一份只包含域名但并没有包含相应 IP 地址的黑名单就可够被绕过去。

③ 代理服务器的可靠性问题：仅使用一个代理服务器来处理所有流进或流出的通信流量可能会引起瓶颈问题，包括速度降低，某些应用程序的失效，甚至是服务器的崩溃。

（2）非技术问题

① ISP（Internet 服务提供商）问题：内容过滤过程中涉及的 ISP 可能会面对很多的问题：包括设置、维护以及管理代理服务器的额外负担，支持和维护被迫使用这些服务器的用户，满足客户需求并充当道德权威的角色（而这个道德权威的角色很难满足所有用户的要求）。除了这些问题之外，ISP 面对的问题还包括如何创建、更新以及托管满足

所有客户需求的黑名单，并且如何以一种安全的方式向客户分配黑名单。

② 创建和维护黑名单的成本：创建和维护一个黑名单的相关成本是非常高的。造成成本如此高的原因主要是黑名单的创建、维护和升级牵涉到本地政治环境的极大变化以及对名单复杂性质的高度理解。除此之外，黑名单是黑客和入侵者的主要攻击目标，因此名单的安全也需要花费很大的成本。

2. 网络层过滤和阻塞

每一个网络包都有源 IP 地址和目的 IP 地址，使得 TCP 协议能够在网络中成功地传输数据包，同时也能对传输错误进行记录。在数据包水平的过滤和阻塞中，过滤实体有一个由“禁止”和“坏”IP 地址组成的黑名单。这个阻塞和过滤过程是通过将所有进入或流出的数据包的 IP 地址和特定的黑名单上的 IP 地址进行比较完成的。然而，由于技术上和非技术上存在的问题，包层次的过滤是有局限性的。

（1）技术问题

① 包层次的过滤是不分差异的：基于服务器 IP 地址的阻塞就意味着来自于内网的任何一台主机都不能到达服务器。也就是说由服务器提供的任何服务都不能被内网用户或受保护的用户计算机所使用。如果用户的意图是阻塞这个网站，这种方法的结果使得内网所有用户或用户 PC 不能到达整个服务器。一种缓和的方法是通过使用端口号来保护网络和用户 PC，这就可以选择性地阻塞服务器上的服务，然而，这个过程可能会影响到代理服务器的性能。

② 路由器容易被绕行：隧道技术就是将一个 IP 数据包隐藏在另一个 IP 数据包中，通常用于分布式虚拟专用网应用以及 IPv4 到 IPv6 的扩展中，可以很容易地把受限制的 IP 地址封装在一个新的 IP 地址数据包中，然后再使用新的 IP 地址将封装之后的数据包在网路中传输。当到达目的地之后，接收者将数据包进行提取得到原始信息。

③ 黑名单上的 IP 地址不容易维护：只要通过查看和比较服务器被访问的次数就能够很容易地确定一台服务器是否已经被列入到黑名单。一旦确定服务器被列入到黑名单，服务器的所有者能够很容易地改变服务器的 IP 地址。基于这个因素，以及新服务器上线和老服务器退役造成的 IP 地址的变化，急需对黑名单列表进行更新。然而，这样做的成本是非常高的。

④ 不规则端口号的使用：尽管不是很常见，但有些应用程序使用不规则的端口号。使用这种不规则的端口号会欺骗服务过滤器，本应该被阻塞的端口号可能会通过过滤器。

（2）非技术问题

增加的操作成本和 ISP 的管理问题：创建、维护以及分配黑名单的成本增量是相当高的。另外，ISP 为了维护一个可被接受的黑名单，必须非常小心地驾驭众多用户文化、宗教以及政治之间的冲突。

10.1.4 过滤内容

针对不同的用户，团体和组织，这份过滤项目的列表是不同的。因为宗教，文化和政治信仰的冲突，几乎不可能提出一个共同的道德准则，并以此来建立黑名单。这就使得社会团体走到一起，建立了一个可被大众接受的共同反对的内容列表。下面给出的这

个列表是从众多资源中收集到的条目。

（1）裸体：不同的文化对裸体的定义不同。然而，在很多文化当中，这意味着完全不穿衣服或者是暴露特定的身体部位。

（2）成人内容：成人内容的定义也是不同的，缺少统一的定义。然而，在许多文化中指被公开分级定义为引起未成年人堕落的内容，可以是粗鲁下流的言语、姿势或行为。

（3）性：根据不同的文化、宗教和政治，性行为的定义也是不同的。

（4）赌博：根据标准的不同，有很多种形式的赌博。这些形式包括实物赌博、在线赌博和游戏赌博。

（5）暴力：引起或造成人类身体或心理上疼痛的所有身体展示的行为，包括谋杀、强奸和折磨虐待。

（6）毒品文化：不论是否是描述性的，提倡非法使用或鼓励非法使用任何消遣性毒品的图形图片，包括香烟和酒的广告。

（7）歧视：提倡对其他民族、宗教、性别、残疾以及国籍的偏见。

（8）邪恶或祭祀：邪恶的内容包含恐怖的信息，可能会导致邪恶的崇拜。

（9）犯罪：对于实施犯罪的鼓励、工具使用的介绍以及提供建议等，包括炸弹的制作和劫持。

（10）低俗：低俗幽默，极端形式的身体修改，如身体切割、烙印、刺穿等。

（11）恐怖主义/好战分子/极端分子：好战，鼓吹侵略行为、极端行为及其他行为。

10.2 病毒过滤

在所有的攻击方式中，病毒是最为流行，危害最为严重的一种方式。本节将重点介绍有关病毒的种类、感染方式、传播途径等内容。

10.2.1 定义

计算机病毒是一种能够进行自动传播并以更改或破坏计算机资源为目的的计算机程序。计算机病毒和自然界的病毒一样，把自己依附在可执行代码上生长、繁殖、传播。当计算机执行代理程序时，病毒也被同时启动，并且在新的环境中进行传播，进而攻击重要的系统资源，包括代理软件本身，计算机中存储的数据，或是计算机硬件，最终使系统崩溃。

病毒一词真正用来指代计算机程序是由 Fred Cohen 开始的，那时他还是南加利福尼亚大学的研究生。Fred Cohen 写了 5 个真正的病毒程序，运行于 UNIX 系统上，当然这些程序并不是为了更改或破坏任何的计算机资源，而是为了进行教学演示。演示过程中，在一个小时的时间内，所有病毒就获得了系统的全部控制权。此后，计算机病毒技术迅猛发展。目前为止，计算机病毒是流行最广，危害性最大，增长速度最快的一种计算机系统攻击形式。据统计，平均每个月就有 400 到 500 种新病毒产生。计算机病毒流行的主要原因包含以下因素。

（1）易产生性。由于计算机代码编写技术的易学性以及互联网上普遍存在的病毒代

码，使得计算机病毒成为所有计算机攻击中最容易实施的一种。

（2）影响范围广。由于全球计算机的高互联性，计算机病毒的传播速度越来越快。“红色代码”病毒的传播速度就证明了这一点。在发行之后的短短几天之内，红色代码就已经传遍了全球网络。

（3）病毒的自动传播性质。比起早期版本的病毒，新型计算机病毒更加危险。新型计算机病毒的自动传播能力其传播速度更快，制造破坏的数量更多。红色代码病毒能够快速传播的一个重要原因就是它的自动传播能力。

（4）病毒变异。变异使得病毒更不容易被清除，并且消耗了巨大的计算机资源。

（5）逮捕病毒开发者的困难性。正如红色代码病毒案例所证明的，由于法律和其他的一些限制，逮捕病毒开发者将变得越来越难，这也造成病毒日益泛滥。

10.2.2 病毒感染方式

计算机病毒感染计算机系统并进行传播的方式有 3 种：引导扇区、宏渗透、寄生虫。

1. 引导扇区渗透

尽管不很常见，但引导扇区依然是培养病毒的一种方式。引导扇区通常是每一块硬盘的第一个部分。在启动盘，这个部分包括了启动计算机的一系列代码。在非启动盘，这个部分包含了文件分配列表（FAT），计算机启动时，这个列表会首先自动被下载到计算机的内存中，并以此创建一个磁盘内容和种类的路标，用于计算机访问磁盘。隐藏在这个部分的计算机病毒就会被下载到计算机内存中。

2. 宏渗透

宏是很小的语言程序，嵌入到代理程序后就能被执行，渗透效率相当高。而且，宏病毒在网络中的繁殖传播速度非常快。造成宏病毒快速传播的能力主要有以下几个方面。

（1）宏应用的不断增加。随着软件技术的不断发展，宏的应用不断增加，通过增加宏功能，用户就可以扩展产品功能。当同时宏也成为病毒入侵和传播的重要工具。

（2）微程序语言的广泛应用。在编写应用程序过程中，微程序语言变得越来越强大，拥有越来越多的功能。例如，VBA 就是这样一种语言，流行的 PowerPoint、Excel 和 Word 中都可以找到由这种语言编写的宏。但同时这也很容易造成病毒的传播。

宏的问题是在 Internet 应用程序中制造了漏洞。例如，VBA 能够被黑客利用在应用程序中定义病毒代码。其他程序或脚本语言构造的宏同样能够很容易地被黑客使用。

3. 寄生虫

这种病毒既不需要隐藏在引导扇区，也不需要一个类似于宏的培养箱。这种病毒将自己依附在一段健康的可执行程序上，当这个程序被执行的时候，病毒也同时被执行。现在，随着互联网的快速发展，这种渗透方法的应用最为广泛，效率也是最高的。这种类型的病毒包括黑色星期五、米开朗琪罗以及冲击波病毒等。

一旦发起病毒攻击，攻击代理就会对目标系统进行扫描以寻找代理主机。如果找到了合适的代理主机，攻击代理会对其进行检测查看是否已经被感染。如果代理主机没有被感染，病毒就会将自己注入到其中，生长、繁殖，等待引起执行的触发事件发生。病毒的任务主要有以下 3 个。

（1）寻找新的环境用以更快地生长，传播。

（2）将自己注入到新发现的机体当中。

（3）植入之后，一种情况是始终保持活跃使得病毒在任何触发事件发生的时候都能被执行，另一种情况是保持暂时的静止直到特殊的事件发生。

10.2.3 病毒感染源

计算机病毒有许多感染源。已知的病毒中，主要有 4 种感染源：移动的计算机磁盘（例如磁盘、软盘、磁带等）；互联网上下载下来的软件（例如测试软件、共享软件、免费软件等）；电子邮件和电子邮件附件；跨平台的可执行程序和脚本。

（1）可移动的计算机磁盘：从可移动计算机磁盘感染的病毒可能是引导区病毒，也可能是磁盘病毒。

- **引导区病毒** 这种病毒攻击硬盘或软盘的引导区。磁盘扇区是磁盘上用于存储数据的一小块区域。对于 DOS 格式化的磁盘，扇区通常是 512 比特长度。尽管对于正常程序磁盘扇区是不可见的，但是由于其构成了计算机使用的数据块，因此对于计算机系统的正确操作是非常重要的。引导区是操作系统运行时所识别的第一个磁盘扇区。之所以称为引导区是因为它包含了每次计算机加电启动时所必须执行的程序。因为其在计算机系统操作的中心作用，对于病毒攻击，引导区是非常脆弱的，经常被病毒利用作为攻击计算机系统其他部分的跳板。使用这种方式，病毒在计算机之间的传播速度是非常快的。引导区病毒同样能够感染硬盘驱动器中的其他磁盘。
- **磁盘病毒** 当病毒不使用引导扇区的时候，就将自己以宏的形式隐藏在硬盘数据或软盘中。宏是嵌入在其他程序中的小程序，并且会在代理程序执行的时候执行。宏病毒通常感染数据和文档文件、模板、电子表格以及数据库文件。

（2）互联网下载的软件：在发展初期，计算机病毒实际上是手工携带的。人们使用软盘携带计算机病毒并进行传播，使其从一台计算机感染到另一台计算机。互联网的发展创造了病毒传播的一个新途径。事实上，现在互联网已经成为计算机病毒传播最快速最主要的途径。互联网下载、公告板、共享软件是携带病毒的真正载体。

（3）电子邮件附件：目前，电子邮件附件是发展最快的一种病毒传播办法。现在 Internet 一大半的通信是由电子邮件构成的，每天都有数以百万计的电子邮件在计算机中被交换，电子邮件通信是使得计算机感染病毒最有效的途径。没有附件的纯文本电子邮件是不会有病毒的，因为纯文本是不能被执行的，所以不能传播病毒（病毒是嵌入在其他可执行文件或应用程序中的可执行程序或宏文件）。

（4）跨平台的可执行程序和脚本：现在 Web 应用非常广泛。 由此产生了诸如 Java、Perl 和 C/C++这样的脚本语言。公共网关接口（CGI）脚本允许开发者在客户端和服务器端创建交互式的 Web 脚本来处理和响应用户的输入。无论是在服务器端运行的 CGI 脚本，还是在客户端用户浏览器上运行的 JavaScript 和 VBScript，都为病毒的进入制造了漏洞。

10.2.4 病毒的种类

按照不同的分类方式，病毒的种类也不同。目前，主要有两种分类方式：基于传播方式的计算机病毒分类和基于结果的病毒分类。

基于传播方式的计算机病毒分类见表 10-1。

表 10-1 基于传播方式的计算机病毒分类

病毒种类	描述
特洛伊木马病毒	特洛伊木马病毒在传播过程中隐藏在编译器、编辑器以及其他常见的用户程序中。一旦安全到达目标系统，当程序被执行时，它就同样可以被执行
多态病毒	这种病毒的特点就是形式变化多。在多态病毒进行复制之前，必须将自己变成其他的形式以避免检测。这也就意味着即使病毒检测者已经知道了病毒的签名，这个签名也是可以改变的。多态病毒也可以对病毒签名进行加密之后再传播，以此躲避防病毒软件。这就使得防病毒工作更加困难。典型的多态病毒有最臭名昭著的“红色代码”病毒，几乎每隔一天就变换一种形式
隐藏型病毒	就像多态病毒为了躲避检查使用变异一样，隐藏型病毒对目标文件和系统的引导区记录进行修改，之后隐藏这些修改。这类病毒往往处在操作系统和应用程序之间。在这些位置，病毒接受操作系统的报告，并且在其传送给应用程序的时候对其进行修改。因此，应用程序和防病毒检测者就很难检测到它的存在。有两种类型的隐藏性病毒：规模隐藏型和读隐藏型。规模隐藏型病毒感染程序之后修改程序的规模，读隐藏型病毒截获对已感染的引导区记录或文件的读请求，提供一个改造的读记录，从而隐藏自身的存在
逆录病毒	逆录病毒攻击目标机器上的防病毒软件，能够关闭防病毒软件，或者能够绕过防病毒软件。另外一种逆转录病毒致力于破坏完整性校验软件中的完整性信息数据库
加壳病毒	这种病毒在目标计算机中首先做的就是保护自己，使得其更难被防病毒软件检测、跟踪、拆解。它病毒使用一层不易被防病毒软件渗透的保护外套。而有些病毒则使用隐藏方式躲避防病毒软件
伴随病毒	这是一种非常聪明的病毒，它首先创建可执行文件，然后在可执行文件的基础之上扩展自己。每次可执行软件启动的时候，这种病毒总是被最先执行
噬菌体病毒	这种病毒可以用自己的代码代替可执行代码。因为这种特性，这种病毒的破坏力非常强大，可以破坏接触到的每一个可执行程序

基于结果的计算机病毒分类见表 10-2。

表 10-2　基于结果的计算机病毒分类

病毒分类	描述
错误生成病毒	这种病毒大多数在可执行软件中启动。一旦被嵌入到软件之中，在这种病毒的作用下，软件就会产生错误
数据和程序破坏者	这种病毒感染软件之后，就把受感染机体作为生长、复制的代理和攻击的踏板，对这个以及其他程序和数据进行破坏
系统粉碎机	这种病毒是杀伤力最强的一种病毒，一旦被引入计算机系统，就会彻底摧毁系统
计算机时间窃取病毒	这种病毒对系统的软件和数据都没有伤害，只是能够窃取系统时间
硬件破坏者病毒	大多数的病毒修改和破坏计算机数据和程序，当然还有一些病毒能够攻击和破坏系统的硬件。这些病毒通常叫做“杀手病毒”。大多数此类病毒将自己依附在微指令或“mic”中，例如 bios 和设备驱动器
逻辑/时间炸弹	逻辑炸弹入侵系统之后，会嵌入到系统软件之中，把系统软件作为代理载体，等待触发事件的发生

10.2.5　病毒防范技术

防病毒技术的目标主要有 4 种类型的病毒：普通（in the wild）病毒、宏病毒、多态病毒以及标准病毒。“in the wild”病毒也就是世界范围内每天在用户计算机上检测到的活跃病毒。

每年，“in the wild”病毒都会被收集并公布在 WildList（WildList，正流行的病毒列表）上。尽管 WildList 不应该被看成最常见病毒的列表，但目前这个列表依然被用作 in the wild 病毒的检测基础，并被许多防病毒软件生产公司作为防病毒产品生产的标准。另外，基于 WildList 上的病毒集合正在被大量防病毒产品检测者用来对常见病毒的命名进行标准化。可以在 http：//www.wildlist.org 上查看到最新的 WildList 列表。

WildLis 于 1996 年 4 月由 Joe Wells 和 Sarah Gordon 共同创建，它是全球三大权威独立评测机构之一，以提供病毒为主，不进行测试。WildList 收集的都是实际发生过感染的病毒，十分贴近用户实际情况，而不是几乎没有生存过的病毒样本。WildList 组织的使命就是为电脑病毒（样本）使用者和防病毒产品开发者，提供“流行在外”的电脑病毒的精确、及时和综合的信息。“WildList”就是那些病毒发生后流行在外的电脑病毒样本清单，由各种组织的超过 55 个符合条件的志愿者发现后并上报来的，然后由“流行病毒清单”组织整理并免费提供给使用者，如图 10-3 和图 10-4 所示。一些反病毒专业人士，志愿的贡献他们的时间和努力，为这个组织提供病毒信息。

其他 3 种类型的病毒已经本节前面的部分讨论过了。防病毒软件致力于检测到所有这些形式的病毒。

```
==============================================================================
                      The Extended WildList - March, 2012
                                 FULL-RELEASE

==============================================================================
 Key Participant             Region         Organization          Product
==============================================================================
 Ao  Amyn Sachedina          USA            Symantec              -
 At  Pavel Krcma             -              AVG Technologies      -
 Bc  Bright Chu              China          FilsecLabs            -
 Dd  Deepen Desai            -              SonicWall             -
 Mg  Grzegorz Michalek       Poland         Arcabit               -
 Pa  Luis Corrons            Spain          Panda                 -
 Pw  Philipp Wolf            Germany        AVIRA                 -
 Rs  Robert Sandilands       USA            Authentium            Command
 Sh  Shali Hsieh             Global         Microsoft             -
 So  SiHaeng Cho             South Korea    Ahnlab, Inc.          V3
 St  Stuart Taylor           UK             Sophos Limited        Sweep
 Ym  Juraj Malcho            -              Eset                  NOD32
==============================================================================
                           The Extended WildList
==============================================================================

 + : new to the list this month.
 * : reappearing entries.

 WildList Entry                                    Reported by:
==============================================================================
 WL-000738ce6c2b6b04915d701d73cd0f96-0             AoYm
+WL-000f3bc70fa19643b464210b116962a3-0             AtShYm
 WL-002d4eb9a4f277be0d7f9ed50757d84c-0             AtYm
 WL-009f8afb4f7dc643662e7b6a0b3e8bfc-0             ShYm
+WL-00f1bc12d7cc6570b706ff1cb1664e1c-0             AoPa
+WL-010b909ffcba74f73a06fa86b0633ef5-0             ShYm
 WL-010ef41c076aaf1b4d80bdd41d42a138-0             PaShYm
```

图 10-3 WildList 网站上公布的病毒列表 1

```
==============================================================================
                                The WildList
==============================================================================
 This main list includes viruses reported by multiple participants,
 which appear to be non-regional in nature. This list is "the" WildList
 according to original specification, which required viruses to be verified
 In-the-Wild by a minimum of two participants.

 After falling off, viruses sometimes reappear on The WildList.  Such
 viruses are denoted with the symbol "*".

 + Viruses marked with a plus sign (+) are new to the list this month.

                                             List  Reported
 Name of Virus                               Date  by:
==============================================================================
 WL-516021e31f3a05ea3a25a502c1d9361a-0      10/11 ShYm
+WL-b91f9e1ac19a021242a87c872b25f893-0       3/12 PaSh
 WL-b3ae8cb2b5e9676a1a39c9b948b5559b-0       1/12 GoShYm
+WL-92ee72bcb7f2acf95dde7b551c29bbfb-0       3/12 PaPwYm
 WL-b8ae4cc30a28c6461956ae341271919a-0       1/12 PaSh
+WL-19f667521f26c787417177a0957da839-0       3/12 MgSh
 WL-95793af07cab513b37f2d240d118c3a3-0      10/11 GoMgSh
 WL-04cedeb4fd1de0343e40f301e4b12d13-0       2/12 GoShYm
 WL-f70b71d63376e7a0823a7d1c67379704-0      10/11 HtShYm
 WL-959f1ce6a71d76e639832a2ac8636626-0      10/11 HtYm
 WL-6256e0bb3bd00abce63f320f4d9c3ff2-0       1/12 PaSh
 WL-db852f21d13ec31c2c4d22f346bd6374-0       2/12 PaShYm
 WL-7978b71587cc793c25c4b08fbf0c84bd-0      10/11 ShYm
 WL-117eff1457c727ef3bee77c6bee477fe-0      10/11 HtYm
```

图 10-4 WildList 网站上公布的病毒列表 2

10.3 垃圾邮件防范技术

10.3.1 垃圾邮件的定义及危害

现在对垃圾邮件还没有一个非常严格的定义。一般来说，凡是未经用户许可就强行发送到用户邮箱中的任何电子邮件都可称为垃圾邮件。在中国，中国电信和中国互联网协会分别对垃圾邮件作了定义。

（1）中国电信对垃圾邮件的定义

2000 年 8 月，中国电信制定了适用于中国电信 IP 网络所有用户（包括拨号用户、专线用户及其他有业务流经中国电信 IP 网的用户）的垃圾邮件处理办法。中国电信将垃圾邮件的定义为："向未主动请求的用户发送的电子邮件广告、刊物或其他资料；没有明确的退信方法、发信人、回信地址等的邮件；利用中国电信的网络从事违反其他 ISP 的安全策略或服务条款的行为；其他预计会导致投诉的邮件。"

（2）中国互联网协会对垃圾邮件的定义

2002 年 11 月 1 日，由中国互联网协会、263 网络集团和新浪网共同发起，中国互联网协会反垃圾邮件协调小组即日在北京正式成立，国内 20 多家邮件服务商首批参加了反垃圾邮件协调小组。媒体称此举是向垃圾邮件打响了第一枪，但枪声响过之后，是否能将目标给予严重打击，目前还看不出任何明显效果。中国互联网协会在《中国互联网协会反垃圾邮件规范》中是这样定义垃圾邮件的："本规范所称垃圾邮件，包括下述属性的电子邮件：收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；收件人无法拒收的电子邮件；隐藏发件人身份、地址、标题等信息的电子邮件；含有虚假的信息源、发件人、路由等信息的电子邮件。"

垃圾邮件可以说是 Internet 带给人类最具争议性的副产品，它的泛滥已经使整个 Internet 不堪重负。其主要危害有以下几点。

（1）占用网络带宽，造成邮件服务器拥塞，进而降低整个网络的运行效率。

（2）侵犯收件人的隐私权，侵占收件人信箱空间，耗费收件人的时间、精力和金钱。有的垃圾邮件还盗用他人的电子邮件地址做发信地址，严重损害了他人的信誉。

（3）成为被黑客利用的工具。2000 年 2 月，黑客攻击雅虎等五大热门网站就是一个例子。黑客首先侵入并控制了一些高带宽的网站，集中众多服务器的带宽能力，然后用数以亿万计的垃圾邮件猛烈袭击目标，造成被攻击网站网路堵塞，最终瘫痪。

（4）严重影响 ISP 的服务形象。在国际上，频繁转发垃圾邮件的主机会被上级国际因特网服务提供商列入国际垃圾邮件数据库，从而导致该主机不能访问国外许多网络。而且收到垃圾邮件的用户会因为 ISP 没有建立完善的垃圾邮件过滤机制，而转向其他 ISP。

因为超过 60%的 Internet 应用是电子邮件应用，因此，垃圾邮件对一大批的 Internet 用户产生作用。有以下几种方式可以用来对抗垃圾邮件。

（1）避免在公共场所张贴电子邮件地址。个人网页底部的电子邮件地址是垃圾邮件制造者的必选目标。如果必须在个人网页上放置个人电子邮件，尝试找一种方式隐藏它。

（2）限制填写要求电子邮件地址的在线表格。如果有可能，就一直避免在填写表格的时候提供电子邮件地址。

（3）使用不容易被猜到的电子邮件地址。现在，垃圾邮件制造者正在试图猜测电子邮件地址，因此尽量使用难以被猜测到的电子邮件地址。

（4）使用多个电子邮件地址。建议同时使用多个电子邮件地址，在个人商业用途上使用一个地址。当填写无关紧要的信息时，使用不同的电子邮件地址。

（5）垃圾邮件过滤。建议在网络层或应用层使用垃圾邮件过滤来阻塞不想要的电子邮件。尽管这种方法存在着一定的问题，但是能够极大地减少用户接受到的垃圾邮件的数量。现在，许多的 ISP 都支持垃圾邮件过滤。

（6）立法。很多国家和地方政府已经通过了打击垃圾邮件的法律。在欧洲，已经通过了欧盟数字隐私规则，并且已经生效。这些条例要求公司在发送电子邮件，在网上获取个人信息，或通过卫星连接的移动电话定位用户之前要先得到用户的同意。这个条例还限制公司使用 cookies 和其他的方法来收集用户的信息。在美国，在联邦政府和州一级政府同样在努力颁布垃圾邮件的法律。除了美国、欧盟、其他一些国家，包括澳大利亚、加拿大、日本、俄罗斯、巴西、印度已经或正在努力颁布垃圾邮件的法律。

10.3.2 反垃圾邮件技术

从 1990 年开始，垃圾邮件就成为网络服务商（ISP）和企业的头号难题。ISP 和企业不得不采取行动来遏制对邮件服务器和网络造成威胁的垃圾邮件。尽管这个问题广泛地被信息行业所承认，但之前却很少有反垃圾邮件的工具和技术。信息行业，包括邮件服务商和相关产品，以及行业标准，对于垃圾邮件问题都反应过慢——最初都低估了垃圾邮件的数量、技术复杂性和影响力。从反垃圾邮件的历史来看，反垃圾邮件技术主要经历了 4 代，如图 10-5 所示。

第一代	第二代	第三代	第四代
基础 MTA 控制 白名单和黑名单 简单的关键字搜索 信件头测试 标题过滤 简单的 DNS 测试	实时黑名单 数字签名	贝叶斯过滤 人工智能 机器语言学习	多技术整合分层过滤

图 10-5 反垃圾邮件技术历史

当前的反垃圾邮件技术主要可以分为 4 大类——过滤技术、验证查询技术、挑战技术和密码术，这些解决办法都可以减少垃圾邮件问题，但是也都存在各自的局限性。

1. 过滤技术

过滤技术是一种相对来说最简单却很直接的处理垃圾邮件技术。这种技术主要用于

接收系统（MUA，如 OUTLOOK EXPRESS 或者 MTA，如 sendmail）来辨别和处理垃圾邮件。从应用情况来看，这种技术也是使用最广泛的，比如很多邮件服务器上的反垃圾邮件插件、反垃圾邮件网关、客户端上的反垃圾邮件功能等，都是采用的过滤技术。过滤技术主要有以下几种类型。

（1）关键词过滤

关键词过滤技术通常创建一些简单或复杂的与垃圾邮件关联的单词表来识别和处理垃圾邮件。比如某些关键词大量出现在垃圾邮件中，如一些病毒的邮件标题，比如：hello。这种方式就像反病毒软件利用病毒特征一样。可以说关键词过滤是一种简单的内容过滤方式来处理垃圾邮件，它的基础是必须创建一个庞大的过滤关键词列表。

过滤技术的缺陷很明显，过滤的能力同关键词有明显联系，关键词列表造成错报的可能性比较大，当然系统采用这种技术来处理邮件的时候消耗的系统资源会比较多。并且，一般躲避关键词的技术比如拆词，组词就很容易绕过过滤。

（2）黑白名单

黑名单（Black List）和白名单（White List）。分别是已知的垃圾邮件发送者或可信任的发送者 IP 地址或者邮件地址。现在有很多组织都在研究 block list，将那些经常发送垃圾邮件的 IP 地址（甚至 IP 地址范围）收集在一起，做成 block list，比如 spamhaus 的 SBL（Spamhaus Block List）可以在很大范围内共享。许多 ISP 正在采用一些组织的 block list 来阻止接收垃圾邮件。白名单则与黑名单相反，对于那些信任的邮件地址或者 IP 就完全接受了。

目前很多邮件接收端都采用了黑白名单的方式来处理垃圾邮件，包括 MUA 和 MTA，当然在 MTA 中使用得更广泛，这样可以有效地减少服务器的负担。

黑白名单技术也有明显的缺陷，因为不能在 block list 中包含所有的（即便是大量）的 IP 地址，而且垃圾邮件发送者很容易通过不同的 IP 地址来制造垃圾。

（3）HASH 技术

HASH 技术是邮件系统通过创建 HASH 来描述邮件内容，比如将邮件的内容、发件人等作为参数，最后计算得出这个邮件的 HASH 来描述这个邮件。如果 HASH 相同，那么说明邮件内容、发件人等相同。HASH 技术在一些 ISP 上比较常用，如果出现重复的 HASH 值，那么就可以怀疑是大批量发送邮件了。

（4）基于规则的过滤

这种过滤根据某些特征（比如单词、词组、位置、大小、附件等）来形成规则，通过这些规则来描述垃圾邮件，就如 IDS 中描述一条入侵事件一样。要使过滤器有效，管理人员必须要维护一个庞大的规则库。

（5）智能和概率系统

这种技术广泛使用的就是贝叶斯（Bayesian）算法，它可以学习单词的频率和模式，这样可以同垃圾邮件和正常邮件关联起来进行判断。相对于关键字来说，这种技术更复杂、更智能化。目前它是客户端和服务器中使用最广泛的技术。

现行的很多采用过滤器技术的反垃圾邮件产品通常都采用了多种过滤器技术，以便使产品更为有效。过滤器通过它们的误报和漏报来分等级。漏报就是指垃圾邮件绕过了过滤器的过滤。而误报则是将正常的邮件判断为了垃圾邮件。完美的过滤器系统应该是

不存在漏报和误报的，但是这是理想情况。

一些基于过滤器原理的反垃圾邮件系统通常有下面的 3 种局限性。

（1）可能被绕过。垃圾邮件发送者和他们用的发送工具也不是静态的，他们也会很快适应过滤器。比如，针对关键字列表，他们可以随机更改一些单词的拼写来绕过 hash 过滤器。当前普遍使用的贝叶斯过滤器可以通过插入随机单词或句子来绕过。多数过滤器都最多只能在少数几周才最有效，为了保持反垃圾邮件系统的实用性，过滤器规则就必须不断更新，比如每天或者每周更新。

（2）误报问题。将正常邮件判断为垃圾邮件是一个比较严重的事故。比如，一封包含单词 sample 的正常邮件可能因此被判断为垃圾邮件。某些正常服务器有时会不幸包含在不负责任的组织发布的 block list 对某个网段进行屏蔽中，而不是由于发送了垃圾邮件。但是，如果要减少误报问题，就可能造成严重的漏报问题。

（3）过滤器复查。由于误报问题的存在，通常被标记为垃圾邮件的消息一般不会被立刻删除，而是被放置到垃圾邮件箱里面，以便日后检查。不幸的是，这也意味着用户仍然必须花费时间去察看垃圾邮件，即便仅只针对邮件标题。

过滤技术可以帮助用户组织并分离邮件为垃圾邮件和正常邮件，但是并不能阻止垃圾邮件，实际上只是在“处理”垃圾邮件。尽管过滤器技术存在局限，但是，这是目前最为广泛使用的反垃圾邮件技术。

2. 验证查询技术

垃圾邮件一般都是使用伪造的发送者地址，极少数的垃圾邮件才会用真实地址。垃圾邮件发送者基于以下几点原因来伪造邮件：因为是违法的，在很多国家，发送垃圾邮件都是违法行为，通过伪造发送地址，发送者就可能避免被起诉；因为不受欢迎，垃圾邮件发送者都明白垃圾邮件是不受欢迎的，通过伪造发送者地址，就可能减少这种反应；受到 ISP 的限制，多数 ISP 都有防止垃圾邮件的服务条款，通过伪造发送者地址，他们可以减少被 ISP 禁止网络访问的可能性。因此，如果能够采用类似黑白名单一样，能够更智能地识别哪些是伪造的邮件，哪些是合法的邮件，那么就能从很大程度上解决垃圾邮件问题，验证查询技术正是基于这样的出发点而产生的。下面介绍的几种都是比较常用的验证查询技术。

（1）反向查询技术

从垃圾邮件的伪造角度来说，能够解决邮件的伪造问题，就可以避免大量垃圾邮件的产生。为了限制伪造发送者地址，一些系统就会要求验证发送者的邮件地址 DNS 是全球互联网服务来处理 IP 地址和域名之间的转化。在 1986 年，DNS 扩展，并有了邮件交换记录（MX），当发送邮件的时候，邮件服务器通过查询 MX 记录来对应接收者的域名。类似于 MX 记录，反查询解决方案就是定义反向的 MX 记录（“RMX”——RMX，“SPF”——SPF，“DMP”——DMP），用来判断是否邮件的指定域名和 IP 地址是完全对应的。因为伪造邮件的地址一般是不会来自 RMX 地址，因此可以判断是否伪造。

（2）DKIM 技术

DKIM（DomainKeys Identified Mail）技术基于雅虎的 DomainKeys 验证技术和思科的 Internet Identified Mail。雅虎的 DomainKeys 利用公共密钥密码术验证电子邮件发件人。

发送系统生成一个签名并把签名插入电子邮件标题，而接收系统利用 DNS 发布的一个公共密钥验证这个签名。思科的验证技术也利用密码算法，但它把签名和电子邮件消息本身关联起来。发送服务器为电子邮件消息签名并把签名和用于生成签名的公共密钥插入一个新标题。而接收系统验证这个用于为电子邮件消息签名的公共密钥是授权给这个发件地址使用的。

DKIM 技术把这两个验证系统整合起来。它以和 DomainKeys 相同的方式用 DNS 发布的公共密钥验证签名，它也利用思科的标题签名技术确保一致性。

DKIM 给邮件提供一种机制来同时验证每个域邮件发送者和消息的完整性。一旦域能被验证，就用来同邮件中的发送者地址作比较来检测真伪，如果是伪造的，那么可能是 spam 或者是欺骗邮件，就可以被丢弃。如果不是伪造的，并且域是已知的，则可为其建立起良好的声誉，并绑定到反垃圾邮件策略系统中，也可以在服务提供商之间共享，甚至直接提供给用户。

（3）SenderID 技术

SenderID 技术主要包括两个方面：发送邮件方的支持和接收邮件方的支持。其中发送邮件方的支持主要有 3 个部分：发信人需要修改邮件服务器的 DNS，增加特定的 SPF 记录以表明其发信身份，比如“v=spf1 ip4:192. 0.4.0/24 –all”，表示使用 SPF1 版本，对于 192. 0.4.0/24 这个网段是有效的；在可选情况下，发信人的 MTA 支持在发信通信协议中增加 SUBMITTER 等扩展，并在其邮件中增加 Resent-Sender、Resent-From、Sender 等信头。

接收邮件方的支持有：收信人的邮件服务器必须采用 SenderID 检查技术，对收到的邮件检查 PRA 或 MAILFROM，查询发件者 DNS 的 SPF 记录，并以此验证发件者身份。

因此，采用 Sender ID 技术，其整个过程如下。

- 发件人撰写邮件并发送。
- 邮件转移到接收邮件服务器。
- 接收邮件服务器通过 SenderID 技术对发件人所声称的身份进行检查（该检查通过 DNS 的特定查询进行）。
- 如果发现发信人所声称的身份和其发信地址相匹配，那么接收该邮件，否则对该邮件采取特定操作，比如直接拒收该邮件，或者作为垃圾邮件。

Sender ID 技术实际上只是一个解决垃圾邮件发送源的技术，从本质上来说，并不能鉴定一个邮件是否是垃圾邮件，所以它不能根除垃圾邮件。垃圾邮件发送者可以通过注册廉价的域名来发送垃圾邮件，从技术的角度来看，一切都是符合规范的；还有，垃圾邮件发送者还可以通过别人的邮件服务器的漏洞转发其垃圾邮件，这同样是 SenderID 技术所不能解决的。

（4）FairUCE 技术

FairUCE（Fair use of Unsolicited Commercial Email）由 IBM 开发，该技术使用网络领域的内置身份管理工具，通过分析电子邮件域名过滤并封锁垃圾邮件。

FairUCE 把收到的邮件同其源头的 IP 地址相链接：在电子邮件地址、电子邮件域和发送邮件的计算机之间建立起一种联系，以确定电子邮件的合法性。比如采用 SPF 或者其他方法。如果，能够找到关系，那么检查接受方的黑白名单，以及域名名声，以此决

定对该邮件的操作，比如接收、拒绝等。

FairUCE 还有一个功能，就是通过溯源找到垃圾邮件的发送源头，并且将那些传递过来的垃圾邮件再转回给发送源头，以此来打击垃圾邮件发送者。这种做法利弊都有。好处就是能够影响垃圾邮件发送源头的性能，坏处就是可能会打击到正常的服务器（比如某些被利用的服务器）的正常工作，同时该功能又复制了大量垃圾流量。

（5）指纹技术

“邮件指纹”技术作为一种反垃圾邮件的新技术越来越受到人们的青睐，这种新的技术给每封发送的电子邮件信息增加扩展了的报头信息。这种报头中会包含一种独特的签名信息，签名信息由相应的加密算法生成，这种算法基于电子邮件用户身份的特有识别信息以及邮件的时间识别信息等。外部电子邮件服务器通常返回原始信息的传输指令，称为“报头信息”，其中包括新指纹的扩展信息和原始信息的一部分。这就允许服务器检测签名信息以确定电子邮件是合法的用户信息还是垃圾邮件制造者的伪造返回消息。其目的是利用邮件指纹组织垃圾邮件风暴。当然这种新技术不可能解决所有问题，但可以保证采用这种技术的邮件服务器免受垃圾邮件的淹没。

上述解决方案都具有一定的可用性，但是也存在一些局限性。

3．挑战技术

垃圾邮件发送者使用一些自动邮件发送软件每天可以产生数百万的邮件。挑战技术通过延缓邮件处理过程，将可以阻碍大量垃圾邮件的发送。那些只发送少量邮件的正常用户不会受到明显的影响。但是，挑战技术只在很少人使用的情况下获得了成功。如果在更普及的情况下，可能人们更关心的是是否会影响到邮件传递而不是会阻碍垃圾邮件。

挑战技术有两种形式：挑战—响应和计算性挑战。

（1）挑战—响应

挑战—响应（Challenge-Response，CR）系统保留着许可发送者的列表。一个新的邮件发送者发送的邮件将被临时保留下来而不被立即传递。然后向这个邮件发送者返回一封包含挑战的邮件（挑战可以是连接 URL 或者是要求回复）。当完成挑战后，新的发送者则被加入到许可发送者列表中。对于那些使用假邮件地址的垃圾邮件来说，它们不可能接收到挑战，而如果使用真实邮件地址的话，又不可能回复所有的挑战。但是，CR 系统还是有许多局限性。

- **CR 死锁问题**　假如 Lily 告诉 Mike 要给朋友 Eric 发送邮件。Mike 发送一个邮件给 Eric，Eric 的 CR 系统临时中断邮件并发送给 Mike 一个挑战。但是 Mike 的 CR 系统又会中断 Eric 这里发送出来的挑战邮件，并发送自己的挑战。因此，结果就是，用户都没有接收到挑战，而且用户也无法回复邮件。而且用户也无法知道，在挑战过程中发生了问题。因此，如果双方都使用 CR 系统的话，他们就可能根本无法进行沟通。
- **自动系统问题**　邮件列表或者那些自动系统，比如一些网站的“发送给同学……”功能，就不可能回应挑战。
- **解释挑战问题**　许多 CR 系统都执行解释性挑战。这些复杂的 CR 系统包含了字符识别和参数匹配，但是即便如此，还是能够进行自动化操作。比如，Yahoo

的 CR 系统在创建新邮件账号的时候，对于那些有简单智能字符分析的系统是存在漏洞的。Hushmail 的邮件 CR 系统要求从蓝背景图片中找出指定的图形（分析背景，找出图形，提交坐标，这是可能的）。

但是实际上，多数的垃圾邮件发送者完全不理睬了这些 CR 系统，因为他们主要是担心没有大量的接收者，而不是担心挑战太复杂。许多垃圾邮件发送者也使用有效的邮件地址。当 CR 系统会干扰垃圾邮件的时候，那些发送者也会找出自动化解决这些挑战的办法。

（2）计算性挑战

目前也提出了一些计算性挑战方案（Computational Challenge，CC），如通过增加发送邮件的“费用”。多数 CC 系统使用复杂的算法来有意拖延时间。对于单个用户来说，这种拖延很难被察觉，但是对于发送大量邮件的垃圾邮件发送者来说，这就意味着要花费很多时间了。CC 系统的实例，如 Hash Cash（http://www.cypherspace.org/adam/hashcash/）。但是，即便如此，CC 系统还是会影响快速通信而不仅影响垃圾邮件。CC 系统存在如下局限。

- **不平等影响** 计算性挑战是以 CPU、内存和网络为基础的，比如，在 1GHz 计算机上挑战可能花费 10 秒，但是在 500MHz 上就需要花费 20 秒了。
- **邮件列表** 许多邮件列表都有数千，甚至数百万的接受者，比如 BugTraq，就可能会被看作垃圾邮件了。CC 系统来处理邮件列表是不现实的，如果垃圾邮件发送有办法通过合法的邮件列表来绕过挑战，那么他们也就有办法绕过其他的挑战了。
- **机器人程序** Sobig 或者其他像垃圾邮件一样的病毒，能让垃圾邮件发送者控制大量的机器，这就让他们能够用大量的系统来均衡“费用”了。
- **合法的机器人程序** 垃圾邮件发送者发送垃圾邮件是因为会给他们带来收入。如果这些人联合起来，就可能提供大量的系统来分担“费用”，这完全是合法的，而且不需要通过病毒手段了。

当前，计算性挑战还没有广泛应用，因为这种技术还不能解决 spam 问题，反而可能干扰正常用户。

4．密码技术

目前，业界提出了采用密码技术来验证邮件发送者的方案。从本质上来说，这些系统采用证书方式来提供证明。没有适当的证书，伪造的邮件就很容易被识别出来，以下就是一些密码解决办法。

目前的 SMTP（简单邮件传输协议）不能直接支持加密验证。一些解决方案扩展了 SMTP（如 S/MIME、PGP/MIME 和 AMTP），还有一些其他的则打算代替现在的邮件体系，比如 MTP。在采用证书的时候，比如 X.509 或 TLS，证书管理机构必须得可用，但是，如果证书存储在 DNS，那么私钥必须得在验证的时候可用，也就是说，如果垃圾邮件发送者可以访问这些私钥，那么他们就可以产生有效的公钥。另一方面，也要用到主要的证书管理机构（CA），但是，邮件是一种分布式系统，没有人希望所有的邮件都由

单独的 CA 来控制。一些解决办法因此允许多个 CA 系统，比如，X.509 就会确定可用的 CA 服务器。这种扩展性也导致垃圾邮件发送者也可以运行着私有的 CA 服务器。

如果没有证书管理机构，就需要其他的途径在发送者和接收者之间来分发密钥。比如，PGP，就可以预先共享公钥。在未连接网络或者比较封闭的群组中，这种办法是可行的，但是在大量个体使用的时候，就不是太适合，特别是对于需要建立新的联系的情况下。从本质上来说，预先共享密钥有点类似白名单的过滤器：只有彼此知道的人才能发送邮件。

但是这些加密解决方案还存在一些缺点，还不能阻止垃圾邮件，主要表现在以下几个方面。

- **滥用自动化工具** 如果在广大范围内被应用，就需要有一种办法为所有用户产生证书或者密钥（包括邮件服务器端，邮件客户端），系统很可能通过一种自动化的方法来提供密钥。可是，可以相信垃圾邮件发送者也会滥用任何自动化系统，并且用来发送经认证的垃圾邮件。
- **可用性问题** 比如，CA 服务器不可用怎么办，邮件被挂起，退票，还是依然可用？垃圾邮件发送者近来对一半以上的提供黑名单网站进行了拒绝服务攻击，并导致这些网站都无法访问。显然，这些垃圾邮件发送者想阻止别人更新黑名单。对于单一的 CA 服务器，很显然也无法避免这样的命运。

其实，现在很多反垃圾邮件方案都不会只单单采取一种技术，而是多种多类技术的综合体。不少国家也在为反垃圾邮件进行立法，以便能够得到法律上的支持。但从技术上来说，这跟反攻击一样，是一个正反双方的博弈过程，一种新的反垃圾邮件技术必然会出现一种对应得垃圾邮件技术，况且，任何一种技术，还没有办法去解决所有问题，技术的发展也将延续下去。

10.3.3 反垃圾邮件典型案例

1. Barracuda 反垃圾邮件网关简介

Barracuda 反垃圾邮件网关及病毒邮件防火墙是一款专业过滤垃圾邮件和病毒邮件的防火墙，它逻辑上部署在邮件服务器前端，对经过的邮件进行 12 层过滤，帮助邮件系统抵御最新的垃圾邮件、病毒邮件、欺诈性邮件、钓鱼邮件、间谍程序邮件等各类邮件威胁，然后将过滤后的正常邮件发送给邮件服务器，达到用户免受垃圾邮件、病毒邮件侵扰的目的。其主要功能和过滤模型如图 10-6 和图 10-7 所示。

2. Barracuda 反垃圾邮件网关部署

Barracuda 反垃圾邮件网关及病毒邮件防火墙支持旁路部署模式，安装方式有两种——MX 记录转发安装方式（在 DNS 上添加新的 MX 记录）和端口转发安装方式（在企业防火墙上使用 NAT 方式将 25 端口指向 Barracuda 反垃圾邮件网关），以下是以端口转发方式来安装 Barracuda 反垃圾邮件网关，如图 10-8 所示。

全面防护		
垃圾及病毒邮件过滤	全局及分用户隔离功能	反退信攻击
SMTP/TLS 加密传输	外发邮件过滤功能	策略遵从
阻止欺诈、钓鱼及恶意软件邮件	12 层过滤模型	
12 层过滤模型		
Dos 防护	速率控制	IP 信誉库（含 Barracuda 信誉防护）
发件人认证	收件人认证	三层病毒防护
用户自定义策略	垃圾邮件指纹分析	意图分析
图像识别	贝叶斯分析	垃圾邮件的规则评分
支持的邮件安全标准		
SPF，DomainKeys	Emailreg.org	支持外部 DNSBL
病毒过滤		
三层病毒防御	Barracuda 实时病毒防护	压缩文件扫描
文件类型阻断		

图 10-6　Barracuda 反垃圾邮件网关主要功能

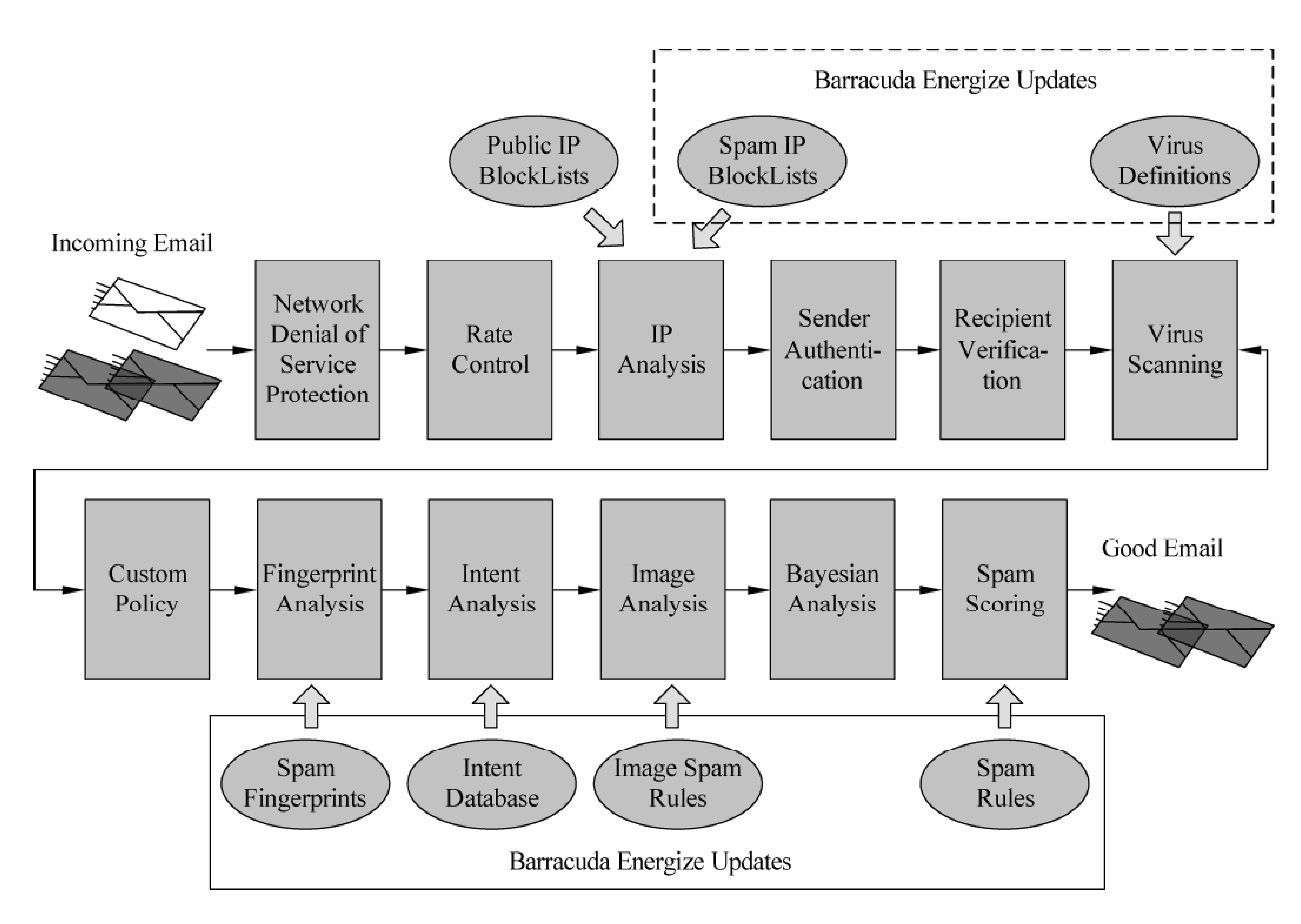


图 10-7　Barracuda 反垃圾邮件网关 12 层过滤模型

邮件流说明如下。

未部署 Barracuda 反垃圾邮件网关前：邮件→防火墙外网出口（25 端口映射给邮件服务器）→邮件服务器。

部署 Barracuda 反垃圾邮件网关后：邮件→防火墙（25 端口映射给 Barracuda 反垃圾邮件网关）→Barracuda 反垃圾邮件网关→邮件服务器。

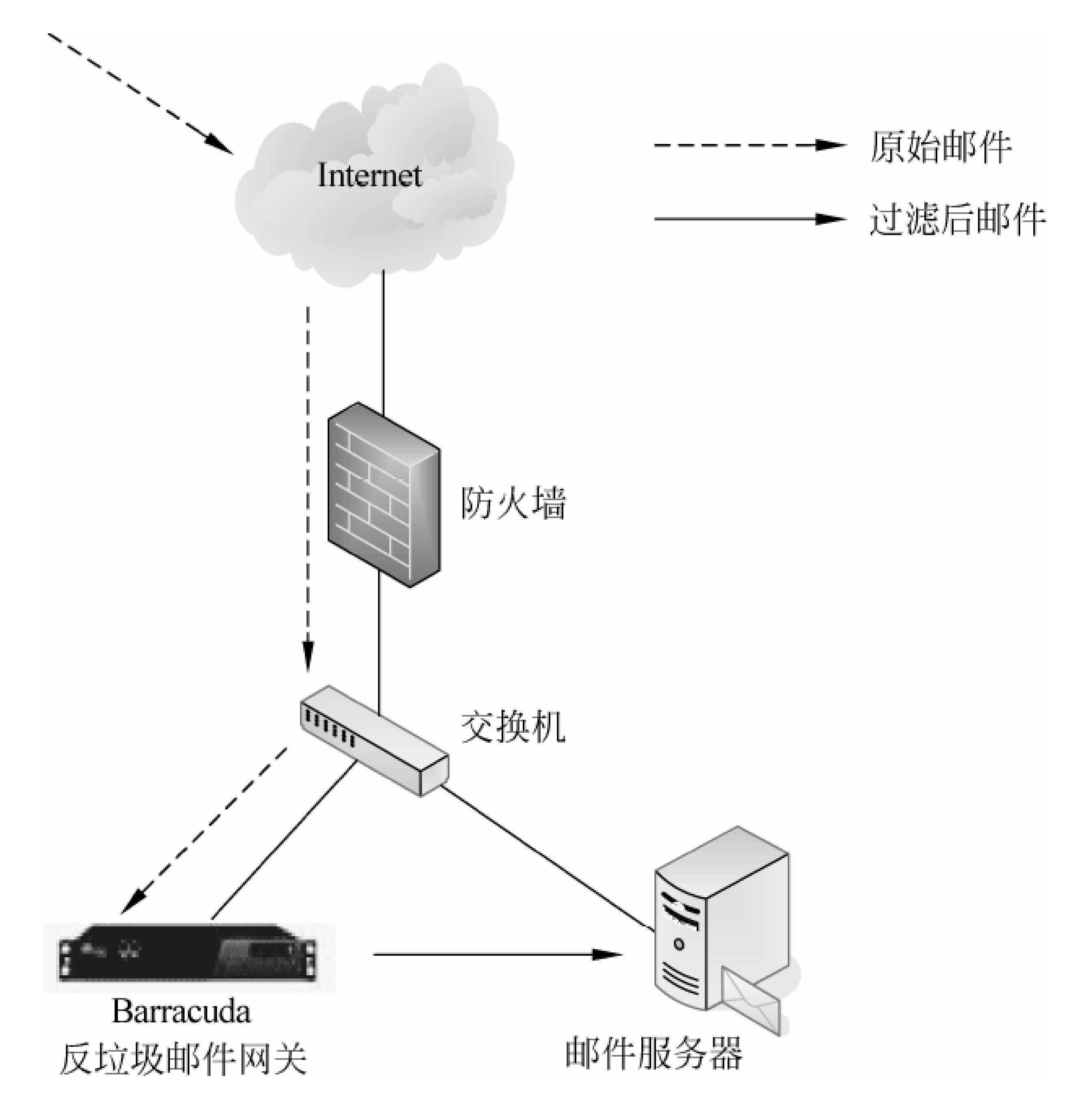


图 10-8 Barracuda 反垃圾邮件网关部署方案（端口转发方式）

习　题

一、选择题

1. 内容过滤发生在哪两个层次？（　　）
   A. 应用层和物理层
   B. 应用层和链路层
   C. 应用层和网络层
   D. 链路层和网络层
2. 病毒感染计算机系统并进行传播的方式有多种，下列哪项不属于此类？（　　）
   A. 引导扇区
   B. 宏渗透
   C. 寄生虫
   D. 移动磁盘

二、简答题

1. 试说明白名单过滤与黑名单过滤的区别。
2. 内容过滤发生在哪两个层次，分别是如何工作的？
3. 简述病毒的种类、感染方式、传播途径。
4. 垃圾邮件有何危害，该如何防范？
5. 反垃圾邮件都有哪些技术，其原理是什么？

课后实践与思考

1. 了解您所在的单位/组织是如何应对垃圾邮件的，其中都运用了哪些反垃圾邮件技术。
2. 登录 WildList 网站了解最新的病毒情况。
3. 了解当前业界流行的防病毒反垃圾邮件技术及方案。

4. Barracuda 反垃圾邮件网关的安装及配置，参考如下示范。

Barracuda 反垃圾邮件网关的安装及配置示范

一、硬件安装

（1）将 Barracuda 垃圾邮件防火墙固定在一个标准的 19 英寸机架或者其他类似地点。



请勿遮挡住机器上方的冷却通风口。

（2）将一根 cat5 网线插到 Barracuda 垃圾邮件防火墙背面网络接口中。Barracuda 垃圾邮件防火墙支持 10MB 或 100MB 网卡，推荐使用 100MB 网络连接。接上标准 vga 显示器及 ps2 键盘。

（3）插上电源线，连通电源。

（4）按下机器面板上的电源按钮。机器前方电源指示灯将点亮，如图 10-9 所示。

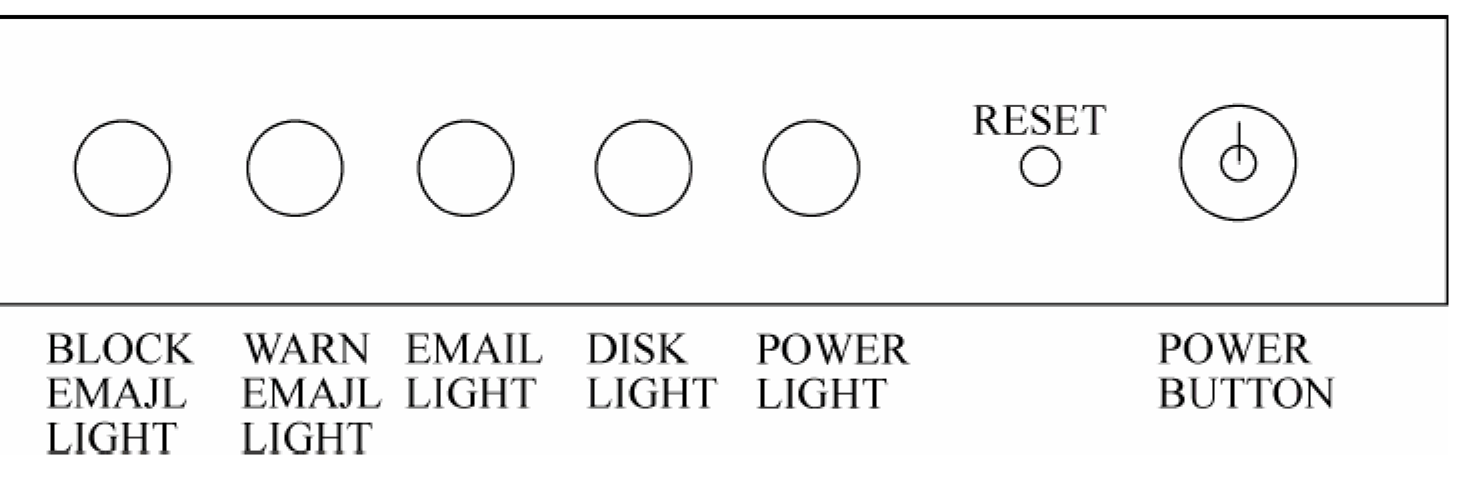


图 10-9　电源指示灯亮

（5）Barracuda 垃圾邮件防火墙前面板上有 5 个指示灯。含义见表 10-3。

表 10-3　指示灯含义

指示灯名	颜色	说明
阻断邮件	红	垃圾邮件或者病毒邮件被阻断时闪烁
警告邮件	黄	标记为垃圾邮件或者隔离时闪烁
邮件	绿	设备收到邮件时闪烁
硬盘	绿	硬盘工作时闪烁
电源	绿	系统接通电源时持续绿灯

（6）reset 按钮有两个功能：重启动机器和复位 Barracuda 到出厂设置。

- ❑ 按 reset 按钮重启动机器。
- ❑ 按住 reset 按钮 5 秒钟将把 Barracudaip 地址设置为 192.168.200.200。
- ❑ 按住 reset 按钮 8 秒钟将把 Barracudaip 地址设置为 192.168.1.200。
- ❑ 按住 reset 按钮 12 秒钟将把 Barracudaip 地址设置为 10.1.1.200。

二、设置 IP 地址

（1）机器启动好后，“barracuda login:”提示显示在显示器上。

- ❑ 输入登录名 admin，密码 admin，如图 10-10 所示。

- ❑ 屏幕将显示目前的系统 IP 配置。
- ❑ 使用 Tab 键，输入新的 IP 地址，网络掩码及默认网关后选择。

```
barracuda login: admin
password:
```

图 10-10　输入登录名和密码

- ❑ 如果需要保存新的 IP 请选择 yes，不保存则选择 no。

三．Web 基本设置

（1）设定系统 IP 地址后，可以从管理界面配置 Barracuda 垃圾邮件防火墙。检查访问的机器与 Barracuda 垃圾邮件防火墙连接在同一个网络中，可以通过 Web 浏览器直接连接到系统 IP 地址。

（2）打开一个 Web 浏览器，输入 Barracuda 垃圾邮件防火墙的 IP 地址，端口为 8000。举例：http://192.168.1.150:8000

（3）进入登录界面，输入用户名 admin，密码 admin。

（4）到基本→IP 设置页，输入所需信息，如图 10-11 所示。



图 10-11　IP 设置

- ❑ 设置 IP 地址、子网掩码及默认网关。
- ❑ 输入目标邮件服务器的名称或地址，输入一个有效的邮件账号测试一下 Barracuda 与邮件服务器的连接。
- ❑ 输入所在网络的 DNS 服务器名称。
- ❑ 输入 Barracuda 垃圾邮件防火墙的主机名和域名。
- ❑ 添加许可的收件人域，除添加好的域之外，Barracuda 将拒绝所有其他域的邮件。

- ❑ 设置完毕请单击“保存”按钮。注意，如果修改了 IP 地址，将与 Barracuda 垃圾邮件防火墙断开，需要用新的 IP 地址登录。

（5）到基本→管理页面进行以下操作。

- ❑ 给 Barracuda 垃圾邮件防火墙指定一个新的管理员密码（可选）。
- ❑ 确定当地的时区选择正确。
- ❑ 单击“保存修改”按钮。

Barracuda 垃圾邮件防火墙现在配置完成，准备过滤所有收到的邮件，并将合法邮件转发到你的邮件服务器上。

四、配置企业防火墙

（1）如果 Barracuda 在企业防火墙之后，需要开放如表 10-4 所示的端口。

表 10-4 开放端口

端口	方向	协议	使用
22	进	TCP	远程检查及服务
25	进/出	TCP/UDP	邮件及邮件弹回
53	进/出	TCP/UDP	域名服务器（DNS）
80	出	TCP/UDP	病毒、固件、垃圾邮件规则库升级
123	进/出	UDP	网络时间协议（NTP）
2703	进/出	TCP/UDP	收到的邮件指纹
6277	进/出	TCP/UDP	收到的邮件指纹

注：只有在远程技术支持时才需要开放 22 端口。

（2）如果您开放了相关端口，您可以立即升级 Barracuda 到最新的版本。进入高级—固件升级页中，下载新的版本，下载完毕之后再按升级。这一过程可能需要几分钟。

五、邮件网关的架设模式

（1）有两种方法：第一种方法称为“端口转发”的安装方式，即在防火墙上设置将 smtp 流映射到 Barracuda 上，Barracuda 过滤好邮件后，再将邮件转发到邮件服务器上。其二，称为“mx 转发”模式，即为 Barracuda 设置一条优先级更高的 mx 记录，这样来自外网的邮件将先发送到 Barracuda 上，Barracuda 过滤好邮件后，再将邮件转发到邮件服务器上。

图 10-12 是“端口转发”安装模式中将 SMTP 指向 Barracuda 的实例：邮件服务器的 IP 是 192.168.1.3，Barracuda 的 IP 是 192.168.1.150，原来的 211.148.5.101 的 SMTP 是映射到邮件服务器上的，Barracuda 架设后，在防火墙上将 211.148.5.101 的 SMTP 改为映射到 Barracuda 上。

mx 转发方式，需要在域名服务器（DNS 服务器）上定义指向 Barracuda 的 mx 记录。用户如果没有自己的 DNS 服务器，可向域名服务商联系。

六、邮件弹回

在阻断垃圾邮件或病毒邮件等情况时，Barracuda 会发送一些弹回信件，用户可以根

据自己的情况选择是否发送，还可以在高级设置→邮件通知编辑中选择适当的弹回邮件模版或自行编辑。



服务	公共IP地址	服务端口	协议	私有IP地址
SSL	211.148.5.101	22	TCP	192.168.1. 150
Web_email	211.148.5.101	8383	TCP	192.168.1. 3
BARRACUDA	211.148.5.101	8000	TCP	192.168.1. 150
POP3	211.148.5.101	110	TCP	192.168.1. 3
SMTP	211.148.5.101	25	Both	192.168.1. 150
DNS	211.148.5.101	53	Both	192.168.1. 3
HTTP	211.148.5.101	80	TCP	192.168.1. 3
FTP	211.148.5.101	21	TCP	192.168.1. 3
msmsgs (192.168.1	0.0.0.0	22013	UDP	192.168.1. 89
msmsgs (192.168.1	0.0.0.0	7915	TCP	192.168.1. 89

图 10-12　SMTP 指向 Barracuda 的实例

七、邮件服务器设置

安装 Barracuda 基本上不需要更改邮件服务器设置，但希望用户能关闭邮件服务器上所有的垃圾过滤控制，以避免潜在的冲突。

八、调整垃圾邮件得分

（1）可以到基础→垃圾邮件得分中设置标记、隔离或阻断得分。阻断得分越低，将过滤更多的垃圾邮件，但可能导致误判率增加。反之则可能导致过滤率减少但误判也减少。因此推荐使用默认设置。

（2）可以设置两种隔离类型：

① 分用户：发送一份个人化隔离报告到个人邮件账户。此报告在每天 3:30 分发送，其中包含一个系统链接，用户可以登录并可以执行以下操作。

- 设置是愿意收到主题行中插入了隔离主题文字的邮件，还是将这些邮件存储在 Barracuda 垃圾邮件防火墙中（默认设置）。
- 是否关闭个人邮箱的垃圾邮件扫描。
- 将发件人邮件地址设置到白名单或黑名单。

② 全局：隔离邮件被发送到指定的通用邮件地址。

九、贝叶斯培训

Barracuda 运行后，对其进行贝叶斯培训可以提高过滤的准确率。贝叶斯数据库中垃圾邮件和非垃圾邮件都超过 200 封后才能生效。建议采用如下的方式进行培训，Barracuda 运行一段时间后在基础→邮件日志中，选择评分大于 7、8 分邮件分类为垃圾邮件；选择评分小于 1 分或 2 分的邮件分类为非垃圾邮件。

第 11 章　信息安全风险评估技术

本章学习重点：

- 理解系统安全策略的作用
- 掌握如何识别信息安全风险
- 掌握信息安全威胁的分析方法
- 掌握系统漏洞的识别与评估
- 了解安全监控与审计

网络与计算机技术的发展推动了操作系统互连互操作的发展，系统之间的互联越来越频繁，互连的程度越来越高，随之伴随的安全问题也日益严重。目前很多大型公司、企业和机构的系统都构建在这些互联互操作的网络之中，实现着资源的共享。

每一个系统都有可能被入侵。系统被入侵后，系统数据可能被破坏或被窃取，因此，必须对网络上的系统进行安全评估。具体来说即首先对风险进行评估，然后根据评估的风险为系统确定合适的安全措施和保护等级。一般评估过程由以下几个部分组成：对系统进行完整的风险、威胁分析；制定合适的安全策略；对系统进行强制性的补丁安装和安全升级。同时，系统在与无安全措施的终端进行资源共享时，还需要一个标准化的规程使风险降到最低。

需要以下几部分完成以上任务。

（1）系统安全策略。

（2）具体特定的安全需求。

（3）风险发现及风险评估。

（4）脆弱性评估。

（5）安全性鉴定。

（6）对漏洞与安全审计的监控。

安全是一个持续的状态，所以确保安全也就是一个持续的过程。首先，需要辨别系统资源面临的安全威胁，通过对系统资源面临的安全威胁进行分析来表示系统的安全漏洞。明确系统安全漏洞之后就可以明确系统具体的安全需求，然后据此制定系统的安全策略。安全策略实施的同时，需要进行审计与监控。这个环节会暴露很多在策略制定过程中遗漏的问题，然后对安全策略进行相应的修改，最后整个过程头尾相连，形成确保系统的安全循环。

11.1　系统安全策略

组织的系统安全对系统管理员是相当重要的。对于任何系统来说，必须对某些请求给予明确的拒绝，这样才能很好地限制网络的主机数、资源和用户的使用权限，从而保护系统的安全。能够公平的情况地完成以上任务的方法就是通过执行一系列的安全策略

来告诉所有的雇员和商业伙伴，在系统中哪些资源是可用的，哪些是不可用的。安全策略也阐明了哪些资源需要被保护以及怎样保护。本质上来说，安全策略是一系列用于规定与限制系统资源使用和所有用户安全责任级别的策略和进程。这样一个机制对组织系统安全是必需的。同时，系统安全策略也影响着系统运行的其他方面，例如以下两个方面。

- **防火墙的设置** 在对一个防火墙进行具体设置的时候，规则库的设置必须参考系统安全策略。
- **用户的使用准则** 在组织中，所有与互联网联接的用户在通过防火墙时都必须遵循安全策略。

安全策略涵盖了整个系统的方方面面，建立安全策略必须将不同的组件都考虑进去，并且将其有机地结合在一起。首先考虑系统的具体需求，然后针对每一个需求提出合适的策略，最后将每一个策略逐步融合在一起，最终形成系统整体的安全策略，而且每一个安全策略都是唯一的，只适用于某个具体的系统。

一个成功的安全策略，应该具备以下几个特性。

（1）能够得最高领导的支持。

（2）能够涉及组织的整个角落和每一个人员，能够明确每个角色在安全系统中应负的责任。

（3）在建立初期，对系统中要保护的内容与保护的原因都有一个清晰的认识。

（4）对于要保护的内容，能够区别优先级。

（5）通过安全策略，能够使组织中的每一个人员明白要保护哪些内容的安全，为什么要保护和怎样保护等问题。

（6）设置一个底线，使用户明白对于系统中的资源，哪些行为是允许的，哪些是不允许的。

（7）由可信的第三方监控执行。

（8）有良好的可扩展性，当有新的规则时能够进行有效地更改。

（9）能够持续有效地运行。

要到达到以上的目标，在建立安全策略的初期就必须遵循以下几个核心步骤。

（1）建立表格对各种共享资源、网络资源进行分类梳理。

（2）对列举出来的资源，分析其所存在的威胁。对每一种威胁，分析出相应的风险，建立一个表格对威胁、风险进行梳理。风险一般有拒绝服务、信息的更改或者泄露、非授权访问。

（3）对所要保护的资源，确定保护的程度。

（4）创建策略小组，其中包括高级管理层、法制部门、IT 部门和文档编辑部门的人员，每个部门至少有一个工作人员出任小组成员，由策略小组负责起草安全策略。

（5）确定需要被审计的内容。一般来说，审计的安全事件一般发生在服务器、防火墙或网络主机上。所以审计的对象一般为服务器、防火墙或网络主机的日志文件，资源存取记录等。

11.2 系统安全要求分析

系统安全要求详细说明组织中每个用户或系统资源的安全特性，人员与资源之间由一个安全访问矩阵连接起来。这些安全要求建立在对目标系统详细了解的基础上。有了对系统的了解之后再来构建由核心安全需求组成的基本架构，然后对每个核心需求进行分析，确定哪些资源需要被保护，为达到安全要求的目标需要采取哪些措施，最后落实措施。

对于安全矩阵来说，有两个核心的实体——用户和资源，通过以下步骤来确定安全需求。

对于用户：包含用户姓名，位置和系统负责人的电话号码，同时还要确定安全忠诚等级，允许访问的用户集，系统用户的最小权限。

对于资源：包含资源的种类，要简要描述正在使用的安全操作系统。如果资源是数据，还应包括以下内容。

（1）保密级别：秘密、机密、绝密。

（2）数据分类：限制访问与严格限制访问。

（3）访问数据的程序。

（4）存取数据所必要的具体访问许可条件。

（5）具体的操作说明。

（6）所有用户的最小特权限制。

11.3 信息安全风险识别

为了理解系统威胁并进行合适的处理，首先必须能够准确地对威胁进行识别。风险识别是一个过程，用于定义并指出资源所面临的威胁，并将威胁按人物或事件进行分类。这些威胁有可能是故意的，也有可能是非故意的。如果一个行为意图破坏客体的安全性，那么该行为就称为故意；而还有一种行为其本身没有破坏客体安全的意图，但存在破坏客体安全性的可能性，则称之为非故意。威胁的来源有很多种，包括人为因素、自然灾害、基础架构故障等，常见的来源有以下几种。

11.3.1 人为因素

人为因素源于人类的感知观念和处理事物能力，其行为有可能增加系统的安全风险，具体来说有以下具体因素。

- **交流**　例如，系统用户与人事部门之间的交流可能导致对策略和用户准则理解的偏差，对专业术语理解的偏差等。
- **人机接口**　很多用户会碰到人性化程度不高的系统接口，在处理这些系统接口时，如果处理不当可能对系统安全产生一定的威胁。
- **数据设计、分析与编码**　当有多数人在场的时候，一定会有可能产生对数据与

设计的曲解，总会或多或少的造成设计失误。

- **新工具与新技术** 当系统有了一些新的工具或新的技术，在使用这些工具、技术时，总会有一定的风险。因为这些对于用于都是陌生的，用户在长期的工具使用中，由于有了原先的惯性，可能在使用过程中操作不当而导致严重的后果。
- **工作负担** 很多系统的用户已经成为了工作负担的受害者，如果这些问题不受重视的话，就会转变成对系统的威胁。
- **工作环境** 工作环境能够在很大程度上影响一个人的心理，感知的敏感度，判断和忍耐能力。而影响工作环境的因素主要包括灯光、噪音、工作站的位置和空间架构。
- **训练** 客观来说，系统内的用户均受过安全训练会对系统安全性起到很有效的作用，因为受过安全训练的用户能够更加安全地使用系统内的设备与技术。

11.3.2 自然灾害

自然灾害导致安全威胁的因素有很多，常见的有地震、火灾、洪水、台风、龙卷风、雷电等。尽管目前无法准确地预测这些自然灾害，但人们能够提前做出准备。同样的，人们也有很多方式应付这些自然灾害，例如异地备份，可以在系统收到损害时短时间内进行数据恢复。

11.3.3 基础架构故障

基础性架构是系统运行的基础，主要包括硬件、软件与管理人员 3 个方面，三者正常的运转缺一不可。此外，三者的每一个环节也很容易出现错，所以基础架构故障属于系统安全风险的主要部分，具体表现在硬件故障、软件故障和人员管理问题这三方面。

1. 硬件故障

经过长时间的发展，计算机的可靠性与原来相比已经有了很大的提升，但硬件故障还是时有发生，这是因为硬件在长期的使用中会有磨损。对于硬件来讲，温度过高、湿度过湿或者灰尘过多都是不适宜的，这容易导致硬件故障。对于硬件故障，有很多方法来应付，包括冗余，也就是说总会有一个备用的系统在准备着，当一个系统突然出现硬件故障而停止工作时，备用的系统就会马上运行保证服务的持续性。还有一个方法就是设置一个监控系统，两个或多个硬件单位持续地相互监控，当检测到其中一个发生故障了，就第一时间报告。另外，硬件技术的进步已经也推进了硬件单元的恢复技术的发展，如果一个组件有发生故障的迹象，那么就会在第一时间使组件停止工作，然后将其负担的计算工作重新分配到其他组件中，并且将故障报告发送给系统中其他组件。

2. 软件故障

目前普遍认为，最严重的安全威胁来自于软件故障。计算机历史上不乏失败的软件项目和软件故障导致重大灾难的例子，如千年恐慌。软件发生运行错误有不同的原因，

有些很明显是人为的错误、软件自身的错误或者软件运行环境的不兼容性。

不管是软件专家还是非专家都明白硬件设计与软件工程是不同的，这些不同也导致了软件的运行故障。

- **复杂性** 不同于硬件设计中易于演示输入时序排列的所有可能，软件设计中即使相同的输入也可能导致数亿种不同的可能输出。所以，在软件设计中不可能演示出所有输出。
- **测试困难** 一段代码可能会存在很多漏洞，但在测试阶段同样不可能将所有的漏洞都测试出来。
- **框架基础设计的误区** 对于基础设计的误区会影响到以后的设计阶段，包括编码、记录和测试，这也导致了软件的主要组件架构不当，对程序中组件不合适的或容易引起歧义的说明等问题。
- **软件升级** 作为软件发展的一个惯例，软件会通过加入一些新的功能或者移除一些漏洞来进行更新换代，但这样更新也会引起一些故障，因为有时新旧版本的编写者不同可能会导致程序的设计风格不同，使用的模块不同，也可能有不同的接口，这些不同带来的差异可能会被一些黑客所利用。
- **管理部门** 很多组织管理部门会有频繁的变动。当一个新的管理者到来时，会关注一些与以往不同的地方，一些新的主管可能会需要一些新的变化，为了适应这些新的变化，就会影响到组织所使用的软件。由于时间与支出的成本问题，很多时候改变都是发生在组织内部。这些改变可能会导致一些新的漏洞、缺陷或出现一些潜在性的威胁。

3. 人员管理问题

人的因素在计算机系统中是很重要的，并且在系统安全中也扮演着至关重要的角色。在硬件系统中，很多时候对某个输入来说，该硬件组件的输出是可以被预测的，当然很多软件的漏洞也是可以被发现并且及时弥补的。但人的因素在计算机系统中就是不可预测的，并且也是不可靠的。人员管理问题一直是计算机安全系统中一个主要的安全威胁。很多影响计算机安全系统的恶意行为都是由用户发动的，这些恶意行为主要有非法入侵系统，或制造能够威胁系统安全的软件。

11.4 信息安全威胁分析

拥有大量资源的信息系统往往是安全威胁的目标。这些系统拥有多于其他系统的价值同时，也存在着大量的安全漏洞，从而也更容易吸引入侵者。所谓信息安全威胁分析就是辨别资源中漏洞的技术，通过持续的检测过程并评估系统安全，然后通过这些得到的信息来对系统进行安全优化。

安全威胁分析的过程包括以下步骤。

（1）确定这些具有较高价值的资源，并进行等级划分。

（2）确定这些资源面临的威胁和威胁来源。

（3）为每一个已选择的资源标识出已知的漏洞，相对而言，已知的漏洞比该资源独

有的安全漏洞更需要对付。

（4）标识出应付这些漏洞所必须的安全机制。

（5）通过对这些资源的安全处理从而加强整个系统的安全。

11.5 信息安全威胁分析方法

目前有多种方法进行安全威胁分析，这些方法一般分为两类：通过计算年预期亏损量进行威胁分析和通过攻击树进行威胁分析两种。

1. 通过定量分析方法进行威胁分析

在介绍年预期亏损量（Annual Loss Expectancy）前，先定义计算预期亏损量是什么。鉴于一个资源被认定为拥有很高的威胁风险，那么当该资源被攻击后，用于替换该资源或恢复该资源所消耗的支出称之为单一预期亏损。威胁风险就是资源的漏洞，通过统计以往的被攻击的次数就可以计算出该资源年预期被攻击概率。

定量分析方法就是利用了这两个基本元素，理论上可以依据其结果计算威胁事件的风险等级，并做出相应的决策。这两个数据就可以用于计算年预期亏损量，具体的公式如下：

年预期亏损量=单一预期亏损×年预期被攻击概率

定量风险方法要求关注的是量化的数据，结果虽然很直观，但这样不能保证数据的完整和可靠。总的来说，信息安全事件的历史数据不多，构建相关的经验模型存在困难，有些威胁不存在频率数据，从而很难准确地把握事件的影响和概率。

2. Schneier 攻击树方法

Schneier 通过使用攻击树的模型来进行风险分析。攻击树就是虚拟地显示可能对目标造成的攻击，攻击树的根节点就是攻击的最终目的，其他的节点就是攻击为了达到最终的目的而必须实行的子步骤。

攻击树是根据攻击的目的添加必要的子目标而成长的，这一步是确定被检查的攻击的细节和复杂程度。如果攻击者必须通过完成这几个子目标才能达成最终的目标，那么如果在攻击树中从叶子节点到根节点的路径越长，说明攻击的复杂度越高。

每一个叶子和相应的子目标都会附加一个相应的支出权值，这样可以显示出达到该目标所需要花费的资源，最经济的路径就是最有可能出现攻击的路径，其威胁也是最大的。

11.6 系统漏洞识别与评估

在系统中一个安全漏洞可能在安全的环境中导致一个安全威胁，这种情况可能演变成系统缺乏安全规程和物理安全控制。尽管安全漏洞很难被预测，但安全漏洞的存在一定会导致系统的不安全性。因此，为了保护计算机系统，人们需要对系统的漏洞进行识

别并评估其危险性。人们也很难在安全事件发生前就能很好地识别所有的系统漏洞。很多时候，只有安全事件发生以后，才能通过该安全事件发现系统的漏洞。对系统漏洞的查找必须面向硬件、软件。值得注意的是，系统漏洞同样存在于系统的安全策略和安全规程之中。

11.6.1 硬件系统漏洞

硬件方面不属于系统漏洞的主要方面，目前很多硬件的漏洞都属于设计、嵌入程序、系统汇编等方面的漏洞。现代计算机与通信系统运行着大量的嵌入式程序，这些程序控制着硬件组件的大多数功能，当这些控制程序出现故障时，硬件也会随之出现不同程度的异常，所以一般而言，硬件漏洞很多时候还是属于软件漏洞，所以本节的讨论重点以软件漏洞为主。

11.6.2 软件系统漏洞

多年以来，在计算机软件中已经发现了不计其数能够削弱安全性的软件漏洞，这给运行软件的系统带来巨大的安全隐患，黑客们完全可以利用某些软件漏洞做任何他们想做的事情。据统计，大多数 IT 安全事件（如网络攻击）都与软件漏洞有关。软件漏洞主要指系统软件、应用软件和控制软件上的漏洞。

1. 系统软件

系统软件是指用于实现系统功能的软件，这些软件属于计算机系统中的核心软件。操作系统中的漏洞比一般的软件漏洞要严重得多。入侵者可以利用这些系统软件漏洞入侵电脑。目前大部分主流操作系统都存在着大量的系统漏洞，这是因为系统软件升级或者添加更多系统功能时，由于对系统软件复杂度了解不够，导致了漏洞的出现。总体来说，越是主流的操作系统，如 UNIX、Linux、MacOS、Windows 等，越容易成为入侵者的目标，因此这些系统的使用率导致了漏洞被发现的概率很高。

2. 应用软件

可以这么说，目前绝大多数的漏洞都是来源于应用软件，原因有以下几点。

（1）相对系统软件，编写应用程序的门槛比较低，目前大部分的应用软件都是一些没有受过系统培训的人编写的。

（2）很多应用软件在完全没有做过测试的情况下就进入市场，造成了潜在的安全威胁。

（3）因为很多软件的编写都目的性很强，很多系统管理者和安全管理者在程序的编写过程中没有起到应有的作用，这样会在接口的扩展性和兼容性方面考虑不周，这些软

件的漏洞可能会对系统的安全造成影响。

（4）软件用了很长时间后，API 和安全工具的发展也会对软件造成安全威胁。重用软件的普遍使用，从其他软件程序中挖取代码模板等也很可能造成软件漏洞。

3．控制软件

控制软件一般为通信协议或者硬件的驱动程序。通信控制程序处于数码模拟设备的核心程序集中，这些程序中的漏洞都会导致网络通信中的数据泄漏。事实上，主流的通信协议集的开放式架构策略中都存在着一些漏洞，目前存在的网络攻击都是由于这些漏洞所引起的。即便这些漏洞被识别，要被修补的难度还是很大的，原因如下。

（1）在某些地方修补已发现的漏洞的支出很大，因为这些地方缺乏相关的知识经验。

（2）尽管有些漏洞在发现以后马上就会有相关的补丁发布，但很多情况下，补丁的速度跟不上发现漏洞的速度，导致目前很多网络攻击都是利用已经被发现的漏洞。

（3）因为整个网络架构是开放式的，所以很多新的组件可以有目的性地添加进入架构中，其兼容性有待完善。

4．策略、规程和实践

系统安全的起点是安全策略和一系列的安全规程。安全策略用于描述系统中用户必须遵守的规范，其在系统安全中起到基础性的作用；而规程从另一方面也阐述了怎样在系统中具体地执行安全策略；实践就是日复一日地去执行规程。除安全策略和规程之外，安全意识也应该在系统安全中体现出来。在考察组织安全策略和规程是否有效时，其效果必须以通过与同类行业对比的形式体现出来。

11.7 安全监控与审计

安全监控是系统安全认证中一个重要的步骤，为了保证持续性的安全监控，控制程序必须放在安全系统之中。安全部门人员和管理人员通过这些控制程序来决定是否需要添加或删减一些步骤来加强系统的安全性。一般来说，监控系统负责做出入侵和异常报告，帮助安全人员迅速确定系统的安全状况，如果系统即将或已经受到损害，安全人员要确定采取何种补救措施。

尽管监控的目标是由安全管理决定，但具体来说，哪些地方需要被监控，哪些信息的日志需要记录，这些都是由管理员或安全管理员决定的。当然安全管理员也可以决定在报告中哪些细节需要被记录才能更好地理解整个系统的安全状态。报告中记录的日志太多或太少都会对随后的分析造成影响。

1．监控工具种类

目前，有多种工具可用于监控系统的状态，一旦选取了一种监控工具，并安装在系统中，其就可以收集能够推断出系统状态的核心信息，并对其进行分析，并直观地表现

出来。在很多系统中，大多数操作系统，如 Windows、UNIX、Linux，监控器可以在事件发生后及时向系统管理员报警。

市面上有大量的监控工具可以使用，一般都是按以下不同用途和需求进行分类。

（1）系统性能：此分类中的监控工具用于主流操作系统性能的日志记录。

（2）网络安全：主要记录了所有入侵检测系统，防火墙等网络安全设备的事件日志。

（3）网络性能和诊断：该类的监控器主要用于监控所有网络行为。

（4）网络连接：用于监控网络的连接状态。

（5）动态 IP 和 DNS 记录。

（6）远程操作与文件共享事件记录。

（7）文件传输工具。

2. 监控工具的功能

目前监控工具一般负责监控、数据收集、信息分析和审计等方面。

- **数据收集**　因为系统运行过程中会有大量的事件产生，所以要在大量的事件中选择合适的事件进行监控尤其重要。很多事件日志记录器会根据相关的条件事先进行相关设置。例如，工作站和服务器，监控系统就会对 CPU 的性能、内存的使用、硬盘的使用、应用程序、DNS 服务器、目录服务器等进行有效监控。另外监控器同样会接受其他系统中的系统日志，如与其连接的服务器、防火墙、路由器等。在网络环境中，日志记录器会通过预先设置的准则对系统用户或系统管理员实时生成报告。
- **信息分析**　系统监控器的目的是捕获系统关键数据并进行分析，分析出有用信息后在合适的时间呈现给系统用户。所以在用户得到该数据前，日志数据必须重新编排并转化成用户可以使用的格式。
- **审计**　审计是计算机系统安全评估的重要工具。与系统监控不同，审计不是持续性的，但其需要的成本和时间支出更大。和监控一样，审计也是预先设置一些准则，然后在事件发生后关注系统的变化。准则的选取应该以能辨别出系统安全是否受损为标准。

一个完整全面的审计应该包含以下几个步骤：①审阅系统起始状态下所有的系统数据；②审阅所有已识别的安全威胁；③选择审计的频率，以日、周或月为单位；④审阅所有的系统行为，确保其没有违背系统准则。

11.8 安全评估工具使用

本章介绍一款免费用于安全评估的工具——Microsoft Security Assessment Tool。其是原 Microsoft Security Risk Self-Assessment Tool (MSRSAT)的修订版本，于 2004 年发行面世，而 Microsoft Security Assessment Tool 2.0 在 2006 年发行面世。该工具采用监视涵盖人员、进程和技术等内容的整体方法来测量系统的安全状态。 以上为 MSAT 软件的官方介绍，这里将对其进行一些简单的使用演示。

首先在 www.microsoft.com 网站上搜索 Microsoft Security Assessment Tool 4.0 即可找到相关信息，然后将对应的软件下载下来，根据相关步骤进行安装，安装成功后进入程序。

（1）进入程序后，由于没有配置文件，所以程序会提醒创建一个新的配置文件，如图 11-1 所示。



图 11-1　创建新配置文件

（2）配置文件创建完成后，会出现一系列的表单待填写，这是对系统整体的认识，依次填写表单完成后，出现“创建新评估”按钮，如图 11-2 所示。



图 11-2　创建新评估

（3）单击“创建新评估”按钮，又会出现一系列表单供填写，这些分别对基础架构、应用程序、运作、人员等方面进行更细致的描述，如图 11-3 所示。

（4）填写完成后，会出现“报表”按钮，如图 11-4 所示。

（5）单击“报表”按钮，就会出现与系统安全相关的信息，如图 11-5 所示。



图 11-3　新评估待填写信息



图 11-4　报表按钮



图 11-5　报表信息

该程序在完整报告中也说明了设计 Microsoft Security Assessment Tool 的目的是帮助用户确定计算基础架构所面临的风险级别以及应对风险已采取的步骤，并提供一些相关建议，但值得一提的是，其不能代替由专业的安全咨询顾问执行的审计。

习　题

一、选择题

1. 可以导致软件运行故障的因素不包括下列哪一项？（　　）
   A. 复杂性
   B. 健壮性
   C. 测试困难
   D. 软件升级
2. 信息安全威胁分析法中，通过使用一种什么样的模型来进行风险分析的计算？（　　）
   A. MD5
   B. Schneier
   C. Hash
   D. Security Assessment

二、简答题

1. 为什么要对系统进行安全风险评估，其基本过程是什么？
2. 什么是系统安全策略，其作用是什么？
3. 为什么人们普遍认为最大的安全威胁就来自于软件故障？
4. 安全威胁分析有哪些常见方法？

课后实践与思考

了解美国信息安全风险评估工作流程

通过参考 NIST SP800 系列标准关于信息安全风险评估的阐述，以下列举了美国政府在实施风险评估和风险控制时的一般流程，具有普遍性，但并不意味着这是固定不变的方法。

1．描述体系特征

在对信息系统的风险进行评估中，第一步是定义工作范围。在该步中，要确定信息系统的边界以及组成系统的资源和信息。对信息系统的特征进行描述后便确立了风险评估工作的范围，刻画了对系统进行授权运行（或认可）的边界，并为风险定义提供了必要的信息（如硬件、软件、系统连通性、负责部门或支持人员）。

本案例所描述的方法学可运用于对单个或多个相关联系统的评估。在评估多个关联系统时，要在运用这些方法学之前就定义好所关心的域、全部接口及依赖关系。

（1）统计系统相关信息

识别信息系统风险时，要求对系统的运行环境有着非常深入的理解。因此从事风险评估的人员必须首先收集系统相关信息，通常这些信息分为如下几类。

- 硬件
- 软件
- 系统接口（如内部和外部连接）
- 数据和信息
- 信息系统的支持和使用人员
- 系统使命（例如信息系统实施的处理过程）

- ❑ 系统和数据的关键性（例如系统对于单位的价值或重要性）
- ❑ 系统和数据的敏感性

与信息系统及其数据的运行环境相关的其他信息还包括（但不限于）以下信息。

- ❑ 信息系统的功能需求
- ❑ 系统的用户（例如为信息系统提供技术支持的系统用户，使用信息系统完成业务功能的应用用户等）
- ❑ 信息系统的系统安全策略（机构策略、政府要求、法律、行业惯例等）
- ❑ 系统安全体系结构
- ❑ 当前的网络拓扑（例如网络图示）
- ❑ 信息系统中的信息流（例如系统接口、系统输入和输出的流程图）
- ❑ 信息系统的安全措施
- ❑ 信息系统的物理安全环境（例如设施安全、数据中心策略等）
- ❑ 针对信息系统处理环境而实现的环境安全（例如对湿度、水、电、污染、温度和化学物品的控制）

对于处在启动或规划阶段的系统，系统信息可以从设计或需求文档中获得。对于处于开发阶段的系统，有必要为未来的信息系统定义关键的安全规则和属性。系统设计文档和系统安全计划可以为开发阶段的信息系统提供有用的安全信息。

对于运行中的信息系统，要从其运行环境中收集信息系统的数据，包括系统配置、连接、流程方面的数据。

（2）信息收集技术

可以使用下列一项或多项技术在其运行边界内获取相关的系统信息。

- ❑ **调查问卷** 要收集相关信息，风险评估人员可以设计一套关于信息系统中的安全措施的调查问卷。可将这套调查问卷发给信息系统的管理和使用人员。调查问卷也可以在现场参观和面谈时使用。
- ❑ **现场面谈** 和信息系统的管理或使用人员面谈有助于风险评估人员收集有用的系统信息（例如系统是如何运行和管理的）。现场参观也能让风险评估人员观察并收集到信息系统在物理、环境和运行方面的信息。
- ❑ **文档审查** 政策文档（例如法律文档、规章等）、系统文档（例如系统用户指南、系统管理员手册、系统设计和需求文档等）、安全相关的文档（例如以前的审计报告、风险评估报告、系统测试结果、系统安全计划、安全策略等）可以提供关于信息系统的安全措施方面的有用信息。对机构使命的影响进行分析或评估资产的关键性后，可以得到系统和数据的关键性和敏感性方面的信息。
- ❑ **使用自动扫描工具** 一些主动的技术方法可以用来有效地收集系统信息。例如，网络映射工具可以识别出运行在一大群主机上的服务，并提供一个快速的方法来为目标信息系统建立轮廓。

信息收集工作可以贯穿于整个风险评估过程，从第 1 步（系统特征描述）一直到第 9 步（结果记录）。

步骤 1 的输出：被评估的信息系统的特征、对信息系统环境的描述、对系统边界的刻画。

2．识别威胁

如果没有脆弱性，威胁源无法造成风险；在确定威胁的可能性时，应该考虑威胁源、潜在的脆弱性和现有的安全措施。

（1）识别威胁源

本步的目标是识别出潜在的威胁源，并且编辑出一份威胁声明，其中要列出被评估的信息系统面临的潜在威胁源。

威胁源被定义为任何可能危害一个信息系统的环境或事件。威胁源按照其性质一般可分为自然威胁和人为威胁。信息系统根据自身应用的特点和地理位置可能会面对不同的威胁源。在评估威胁源时，要考虑可能危害信息系统及其处理环境的所有潜在威胁源。

（2）动机和行为

攻击的动机和资源使得人成为了潜在的危险威胁源之一。表 11-1 概括了许多常见的人为威胁、其可能的动机、可能的攻击方法和威胁行为。这些信息对一个单位研究其面临的人为威胁环境并制定人为威胁声明非常有用。另外，以下方法也有助于标识人为威胁：审查系统的破坏历史、安全违规报告、事故报告；在信息收集过程中与系统管理员、技术支持人员、用户面谈。

表 11-1　人为威胁的威胁源、动机和威胁行为

威胁源	动机	威胁行为
黑客	挑战	破解
	自负	社会工程
	反叛	系统入侵、闯入
		未授权访问
计算机罪犯	破坏信息	计算机犯罪（例如网络骚扰）
	非法泄漏信息	欺诈行为（例如重放、身份假冒、截获）
	非法篡改数据	伪造
	获取钱财	系统入侵
恐怖分子	勒索	炸弹/恐怖主义
	破坏	信息战
	恶意利用	系统攻击（例如分布式拒绝服务）
	复仇	系统渗透
		系统篡改
工业间谍	竞争优势	信息窃取
	经济间谍	侵犯个人隐私
		社会工程
		系统渗透
		未授权的系统访问

续表

威胁源	动机	威胁行为
内部人员 （没有接受良好培训、心怀不满、恶意、疏忽、不诚实、离职员工）	好奇 自负 聪明 获取钱财 复仇 无意错误和疏忽（例如数据录入错误、编程错误）	骚扰员工 勒索 浏览专属信息 计算机滥用 欺诈和窃取 信息贿赂 输入伪造的、被破坏过的信息 截获 恶意代码（例如病毒、逻辑炸弹、特洛伊木马） 出卖个人信息 系统缺陷 系统入侵 系统破坏 未授权系统访问

为了确定脆弱性被利用的可能性，在识别出潜在的威胁源后，要对其发起一次成功攻击所需的动机、资源和能力做出估计。

应该为单位及其处理环境制定威胁声明或潜在威胁源的清单。关于威胁的信息来源一般包括（但不限于）以下几方面。

- 信息咨询机构。
- 件响应或应急响应中心。
- 大众媒体，尤其是基于 Web 的资源，例如安全网站。

步骤 2 的输出：威胁声明，其中包括对威胁源的记录，该威胁源可能会利用系统的脆弱性发动攻击。

3. 识别脆弱性

本步的目标是制定系统中可能会被威胁源利用的脆弱性（缺陷或薄弱环节）的列表。表 11-2 中列出了一些脆弱性/威胁对的例子。

表 11-2 脆弱性/威胁对

脆弱性	威胁源	威胁行为
离职员工的系统账号没有从系统中注销	离职员工	拨号进入单位网络，并访问公司的敏感数据
单位的防火墙允许进入方向的 telnet，并且在某服务器上允许以 guest 账号进入	未经授权的用户（例如黑客、离职员工、计算机罪犯、恐怖分子）	通过 telnet，用 guest 账号进入某服务器，浏览系统文件
厂商在系统安全设计中存在为人所知的缺陷，但还没有补丁文件	未经授权的用户（例如黑客、离职员工、计算机罪犯、恐怖分子）	基于已为人所知的系统的脆弱性，未授权地访问敏感的系统文件
数据中心使用洒水器来灭火，没有用防水油布来保护硬件和设备	火灾、人员疏忽大意	打开了数据中心的洒水器

识别系统脆弱性可以有以下几种建议的方法：使用脆弱性源，测试系统安全性能，以及制定安全要求核对表。

（1）脆弱性源

可以用系统安全测试技术来识别信息系统处理环境中的技术和非技术脆弱性。对其他资源（例如标识系统缺陷和 Bug 的厂商 Web 主页）进行检查也有好处，这些手段可以用来标识某些特定的信息系统（例如特定操作系统的一个具体版本）的脆弱性。Internet 上也可查询到各方面发布的脆弱性修复办法、服务包、补丁文件以及其他可消除或减缓脆弱性的矫正措施。所记录下的系统脆弱性源将得到全面的分析，这些脆弱性源包括（但不限于）以下内容。

- 信息系统在以前经过的风险评估的文档
- 信息系统审计报告、系统异常报告、安全检查报告、系统测试和评价报告等
- 脆弱性列表
- 软件安全分析

（2）系统安全测试

基于信息系统的关键性和可用的资源（例如所分配的资金、可以获得的技术、测试人员所掌握的技术），可以采用系统测试等主动方法来有效地识别系统的脆弱性，这些测试方法包括以下几种。

- 自动化脆弱性扫描工具
- 系统测试和评估（ST&E）
- 渗透性测试

自动化的脆弱性扫描工具可用来对一组主机或一个网络进行扫描，以找出已知的脆弱性。但是要注意到有些由自动化脆弱性扫描工具识别出来的可能的脆弱性可能无法表示系统环境中的真实脆弱性。例如，某些扫描工具在对脆弱性评级时，没有考虑现场的环境和需求。有些由这类扫描工具标记出来的脆弱性在特定现场可能并不是真正的脆弱性，而不过是它们所在的环境要求这样配置罢了。因此这种测试方法可能会产生误报。

ST&E 是另一种用来在风险评估过程中识别信息系统脆弱性的技术，它包括制订并执行测试计划（例如测试脚本、测试流程和预期的测试结果）。系统安全测试的意图是测试信息系统的安全措施在运行环境中的有效性，其目的是保证所采用的控制满足了已获批准的软件和硬件安全规范，并实现了机构的安全策略和业界标准。

渗透性测试可以用来补充对安全控制的检测，并保证信息系统的各个不同方面都是安全的。当在风险评估过程中采用渗透性测试时，可以用它评估信息系统对故意规避系统安全的攻击进行抵御的能力，其目的是从威胁源的角度来对信息系统进行测试，以识别出信息系统保护计划中可能被疏忽的环节。这类可选安全测试的结果将有助于对系统脆弱性的识别。

步骤 3 的输出：有可能被潜在的威胁源所利用的系统脆弱性（观察报告）清单。

4．分析安全控制

本步的目标是对已经实现和计划实现的安全措施进行分析——单位通过这些措施来减小或消除一个威胁源利用系统脆弱性的可能性（或概率）。

要产生一个总体的可能性级别评定，以说明一个潜在的脆弱性在相关威胁环境下被攻击的可能性，便需要分析当前已经实现的安全措施。例如，如果威胁源的兴趣或能力级别很低，或者通过有效的安全措施可以消除或减轻危害的后果，那么一个脆弱性（例如系统或流程中的薄弱环节）被利用来发动攻击的可能性就低。

（1）安全措施

安全措施包括对技术和非技术措施的运用。技术类措施是那些融入到计算机硬件、软件或固件中的保护措施（例如访问控制机制、标识和鉴别机制、加密方法、入侵检测软件等）；非技术类措施包括管理和运行类措施，例如安全策略、操作流程、人员、物理和环境安全。

（2）安全措施的分析技术

制定安全要求核对表或使用一个已有的核对表将有助于以一种有效且系统化的方式对安全措施进行分析。安全要求核对表可以用来验证安全是否与既有的法规和政策相一致。因此，在单位的控制环境发生变化（例如安全策略、方法和要求发生变化）后，有必要对核对表进行更新，以确保其有效性。

步骤 4 的输出：信息系统已经实现的控制清单。

5. 分析可能性

这个步骤要说明一个潜在的脆弱性在相关威胁环境下被攻击的可能性，下列支配因素应该在本步中考虑。

（1）威胁源的动机和能力。

（2）脆弱性的性质。

（3）安全措施的有效性。

一个潜在的脆弱性被一个给定威胁源攻击的可能性可以用高、中、低来表示。表 11-3 描述了这 3 个可能性级别。

表 11-3　可能性的定义

可能性级别	可能性描述
高	威胁源具有强烈的动机和足够的能力，防止脆弱性被利用的安全措施是无效的
中	威胁源具有一定的动机和能力，但是已经部署的安全措施可以阻止对脆弱性的成功利用
低	威胁源缺少动机和能力，或者已经部署的安全措施能够防止（至少能大大地阻止）对脆弱性的利用

步骤 5 的输出：可能性级别（高、中或低）。

6. 分析影响

度量风险级别的下一主要步骤便是确定对脆弱性的一次成功攻击所产生的负面影响。在开始影响分析过程之前，有必要获得以下信息。

（1）系统使命（例如信息系统的处理过程）

（2）系统和数据的关键性（系统对单位的价值和重要性）

（3）系统和数据的敏感性

这些信息可以从现有的文档中获得，例如使命影响分析报告或资产关键性评估报告。使命影响分析将根据对资产关键性和敏感性的定量或定性评估而对单位资产面临的破坏级别进行排序。资产关键性评估活动将对关键或敏感的信息资产（例如硬件、软件、系统、服务以及相关的技术资产）进行标识和排序，是这些资产支持了单位的关键使命。

如果没有这些文档，或对单位信息资产的类似评估还没有开始进行，则可以根据系统和数据的可用性、完整性和保密性保护级别来确定其敏感性。不管用何种方法来确定敏感级，系统和信息的所有者都要负责判断其系统和信息可能遭到的影响级别。因此，在分析影响时最好同系统和信息的拥有者商谈。

对安全事件的负面影响可以用完整性、可用性和保密性 3 个安全属性的损失或降低来描述。下面列出了每个安全属性的简要描述以及它们未被满足后可能带来的后果（或影响）。

- ❑ **完整性损失** 系统和数据的完整性是指要求对信息进行保护，防止其遭到不适当的修改。如果对系统和数据进行了未授权（无论是有意还是无意的）的改动，则完整性便遭到了破坏。如果对系统或数据的这种完整性损失不加以修正，继续使用被感染的系统或被破坏的数据，便有可能会导致不精确性、欺诈或错误的决策。此外，对完整性的破坏往往是对可用性和保密性进行成功攻击的第一步。
- ❑ **可用性损失** 如果一个关键的信息系统对其端用户是不可用的，那么单位的使命就会受影响。例如，系统功能和有效性的损失可能会延误生产时间，因此便妨碍了端用户的功能发挥。
- ❑ **保密性损失** 系统和数据的保密性是指对信息进行保护，防止未经授权的泄露。保密信息的未授权泄露带来的影响范围很广，可以从破坏国家安全到泄露隐私数据。未授权的、非预期的或故意地泄露信息有可能会导致公众信心的下降、难堪或使机构面临法律诉讼。

有些有形影响可以通过营收损失、修复系统的成本、修复由破坏而引发的问题所需要的努力程度等定量测出。其他影响（例如公众信心损失、信用损失、单位利益的破坏）则不能用具体的数量单位来度量，而只能通过定性手段进行度量，或用高、中、低影响等术语来描述，见表 11-4。

表 11-4 影响级别的定义

影响级别	影响定义
高	对脆弱性的利用：①可能导致有形资产或资源的高成本损失；②可能严重违返、危害或阻碍单位的使命、声誉或利益；③可能导致人员死亡或严重伤害
中	对脆弱性的利用：①可能导致有形资产或资源的损失；②可能违反、危害或阻碍单位的使命、声誉或利益；③可能导致人员伤害
低	对脆弱性的利用：①可能导致某些有形资产或资源的损失；②可能对单位的使命、声誉或利益造成值得注意的影响

在进行影响分析时，应该考虑定性和定量评估的优缺点。定性影响分析的优点是它可对风险进行排序并能够对那些需要立即改善的环节进行标识。定性影响分析的缺点是

它没有对影响大小给出具体的定量度量，因此使得成本效益分析变得很困难。

定量影响分析的主要优点是它对影响大小给出了度量，使得可以用成本效益分析来控制成本。缺点是它依赖于用来表示度量的数字范围，定量影响分析的结果的含义可能因而会比较模糊，还要以定性的方式对结果做解释。在确定影响大小时还经常要考虑其他因素，包括（但不限于）以下几个方面。

（1）对威胁源在一段时间内（例如一年）利用脆弱性的频率进行估计。

（2）威胁源每次利用脆弱性发起攻击时的近似成本。

（3）经过对一次特定影响进行主观分析后给出的加权因素。

步骤 6 的输出：影响大小（高、中或低）。

7．确定风险

这一步的目的是评估信息系统的风险级别。确定一个特定的威胁/脆弱性对带来的风险时，可以将其表示为以下参数构成的函数。

（1）给定的威胁源试图攻击一个给定的系统脆弱性的可能性。

（2）一个威胁源成功攻击了这个系统的脆弱性后所造成的影响的程度。

（3）规划中或现有的安全措施对于降低或消除风险的充分性。

为度量风险，首先必须制定一个风险尺度和风险级别矩阵。

（1）风险级别矩阵

将威胁的可能性（例如概率）及威胁影响的级别相乘后便得出了最终的使命风险。下面是一个关于威胁的可能性（高、中、低）和威胁影响（高、中、低）的 3×3 矩阵。根据现场要求和风险评估要求的粒度，有些情况下也可能使用 4×4 或 5×5 的矩阵，后者可以包括一个很低/很高的威胁可能性和一个很低/很高的威胁影响，从而产生一个很低/很高的风险级别。“很高”的风险级别可能要求系统关闭或停止所有的信息系统集成及测试工作。

表 11-5 中的矩阵范例描述了高、中或低的总体风险级别是如何得出的。这种风险级别或等级的确定可能是主观性的。这种判断的基本原理可以用每个可能性级别上分配的概率值和每个影响级别上分配的影响值来解释。例如：①赋给每个威胁可能性级上的概率为 1.0 时表示高，0.5 表示中，0.1 表示低；②赋给每个影响级上的值为 100 时表示高，50 表示中，10 表示低。

表 11-5　风险级别矩阵

威胁可能性	影响		
	低（10）	中（50）	高（100）
高（1.0）	低 10×1.0 = 10	中 50×1.0 = 50	高 100×1.0 = 100
中（0.5）	低 10×0.5 = 5	中 50×0.5 = 25	中 100×0.5 = 50
低（0.1）	低 10×0.1 = 1	低 50×0.1 = 5	低 100×0.1 = 10

风险尺度：高（50～100）；中（10～50）；低（1～10）。

（2）风险级别描述

表 11-6 描述了上述矩阵中的风险级别。这种表示为高、中、低的风险尺度代表了如

果给定的脆弱性被利用来攻击时，信息系统、设施或流程可能暴露出的风险程度或级别。风险尺度也表示了高级管理人员和系统拥有者对每种风险级别必须采取的行动。

表 11-6　风险尺度和必要行动

风险级别	风险描述和必要行动
高	如果被评估为高风险，那么便强烈要求有纠正措施。一个现有系统可能要继续运行，但是必须尽快部署针对性计划
中	如果被评估为中风险，那么便要求有纠正行动，必须在一个合理的时间段内制订有关计划来实施这些行动
低	如果被评估为低风险，那么单位的管理层就必须确定是否还需要采取纠正行动或者是否接受风险

步骤 7 的输出：风险级别（高、中、低）。

8．建议安全措施

在这一步里，将针对单位的运行提出可用来控制已识别出的风险的安全措施。这些措施的目标是降低信息系统的风险级别，使其达到一个可接受的水平。在对安全措施以及减缓或消除已识别风险的备选方案提出建议时，应该考虑下列因素。

（1）所建议的选项的有效性（如系统的兼容性）

（2）法律法规

（3）单位的政策

（4）对运行的影响

（5）安全性和可靠性

建议安全措施是风险评估过程的结果，并为风险控制过程提供了输入。

步骤 8 的输出：减缓风险的安全措施建议及备选解决方案。

9．记录评估结果

一旦风险评估全部结束（威胁源和系统脆弱性已经被识别出来，风险也得到了评估，安全措施建议也已经提出），该过程的结果应该被记录到正式的报告或简报里。

步骤 9 的输出：风险评估报告，它描述了威胁和脆弱性和风险度量，并为安全控制的实现提供了建议。

第 12 章　灾难备份与恢复技术

本章学习重点：

- 理解系统灾难的含义
- 理解系统灾难预防响应的含义
- 了解如何制定灾难恢复计划

一般来说，灾难指能够对社会造成影响的突然的灾害，其产生原因可能来自于人类自身也可能来自于自然。人为的因素包括恶意破坏、操作失误、疏忽大意等。自然因素包括台风、龙卷风或海啸等。这些因素都有可能导致信息系统严重故障甚至瘫痪，有的影响是暂时的，有的却是长期的。灾难管理技术就是为了减缓这些影响而产生的。

在信息技术中，灾难对所有企业信息系统来说都是一个不可回避的安全问题。为了使组织保持竞争力，所有通信系统都必须保持 24 小时持续工作。当灾害来临时，如果系统不能承受这些影响而导致崩溃，那也就意味着该系统在商业方面的失败。特别是在 9·11 袭击以后，很多公司与企业都认识到了灾难管理的重要性。

目前灾难管理的重点主要在于灾难预防、灾难响应与灾难恢复。本章将灾难管理当作信息系统主要的安全问题，并讨论了灾难处理的方式、工具与实践。

灾难分为自然因素与人为因素两种，其中自然因素主要包括台风、龙卷风、洪灾、冰雪天气、泥石流、干旱、地震、地磁风暴、雪灾、火灾等，而人为因素主要包括暴力袭击、蓄意破坏、盗窃、病毒、蠕虫、恶意代码、战争、纵火、网络犯罪等。

12.1　灾难预防

所谓灾难预防就是通过采取一系列由控制策略组成的前置措施确保灾难不会发生。控制者有可能是一个人或一个机制甚至是一个数字传感器设备。随着技术的发展，灾难预防与灾难恢复的技术也在提升。灾难预防的作用就是及时检测异常情况，使工作人员可以有时间应对即将到来的危机。例如在机房内设有温度指示器，其显示机房内温度上升异常，那么就可以在火灾发生之前将计算设备关闭。

在过去的一段时间里，系统灾难预防很大程度上依赖于人员的能力，通过个人经验对不常见的环境进行检测、判断。例如高温、烟雾的出现，设备的断电等情况都有可能造成信息系统的损坏。

随着技术的发展，各种智能监控设备已经应用在灾难预防过程中。监控设备可以对由灾难事件引起的系统不常见变化做出迅速反应。目前，监控设备可以监控以下环境：温度、湿度、雨水、烟雾、风速、访问控制安全、系统报警器状态等，还包括一些不容易被工作人员发现的隐蔽位置，如空调管道、升降梯下面等。

监控过程中，如果有灾难发生的信号出现，就会马上触发行动模块。具体采取的行

动由系统管理员预先设定，包含以下内容。

- 运行本地或远端报警指示器，如汽笛、铃铛、光信号或人工合成声音。
- 隔离受影响的资源，将能量供给切断或保持低能量供给。供给线可能为电源、水源、燃料或其他一类东西。
- 给相关人员发送信号，包括系统用户、管理员、安全人员、维护人员、通过认证的远程用户。
- 以上一个或多个操作完成后，系统将会等待响应。

12.2 系统灾难响应

灾难响应是针对受影响的团体进行长期或短期的处理来降低影响程度的一系列策略。在处理灾难响应时，策略的执行必须快速及时。通常来说，大体上分为两个步骤：快速响应和灾难恢复。

快速响应的关键因素

灾难发生后，及时快速的响应对于减少系统损失，使系统迅速恢复正常工作起到了重要作用。下面列出了影响系统能否做出快速响应的几个关键因素。

- **灾难发生后造成的风险种类** 如果事前遇到过相似问题，响应的效率会大幅提高。
- **灾难发生的环境** 灾难发生的环境决定了需要做出何种响应，要列出清单，标明房间内的物品种类及系统位置。
- **可用资源的数量** 灾难响应有效性取决于当场可用的资源数量，这些资源有助于提高响应的成功率。
- **采取响应行动的时间** 灾难响应中，时间决定了可以采取多少行动以及可以在多大程度上控制灾难影响。
- **对于执行策略的理解** 每种响应方案都应遵循组织的安全策略，对策略的正确理解可以有效提高灾难响应的有效性。

一个优秀灾难恢复计划的价值在于其可快速做出反应并有效减小威胁。为实现这一目的，3 个因素必不可少：消息灵通的工作小组、资源提供商和确定的程序。当然计划不是写在纸上就束之高阁了，还需要进行周期性的排练。例如，在 9•11 恐怖袭击后，美国的企业都认识到了离线备份数据的重要性。因此在袭击以后，定期对离线存储设备中的数据进行检索就成为了一种常态。

制订灾难恢复计划是一个需要细心对待的复杂过程，包含了风险评估、计划制订、文档编排、计划执行、测试和维护等一系列步骤。计划制订之初，应该由灾难恢复委员会的多个成员共同进行，因为这些成员来自于组织内的不同部门，能够决定灾难发生时需要提供恢复的具体解决方法。制订计划的过程由多个步骤组成，具体包括以下步骤。

（1）识别存在的灾难，并设定优先级。

（2）识别系统的核心功能并设定优先级。
（3）识别系统的核心资源并进行威胁分析。
（4）制订告知计划。
（5）制订伤害评估计划。
（6）设定灾难恢复站点。
（7）制订用于在灾难恢复站点进行核心功能恢复的计划。

由于灾难是不可预估的，通常具有不确定性与不可预知性，因此灾难恢复计划需要持续运行，作为一个动态进程始终贯穿在系统的生命周期之中。

12.3 灾难恢复委员会

灾难恢复委员会主要负责制订并修改灾难恢复计划，委员会需要了解系统中每个部门的功能和核心的商业单元，防止在制订计划时遗漏系统的核心信息和资产。委员会的所有成员都应进行有关灾难恢复的训练，每个成员都应被赋予识别各自部门关键行为的责任，委员会同样担任着对其他员工传输安全意识的责任。

12.4 恢复进程

灾难管理与恢复的下一步措施是采取各种实际方法来减轻灾难造成的损害。这主要包括以下几个过程：识别灾难并设定优先级、标记核心资源、制订通告计划和组织员工培训等。

1．识别灾难并设定优先级

灾难造成的影响一般分为低、中、高 3 个层次。

- **低级灾难**　人为误操作、室内高温、服务出错。
- **中级灾难**　病毒攻击、长时间的停电、服务器故障。
- **高级灾难**　地震、海啸、大火、恐怖袭击。

2．标记核心资源

核心资产的排名基于设备本身所要花费的与破坏后恢复所需花费的金钱总数量。这些核心资产包括：服务器、工作站和外设；应用程序和数据；电信连接；物理架构（电力，环境控制）。

根据以上标准进行如下排名。

- **低级资源**　打印纸、打印墨盒、笔和桌子等。
- **中级资源**　工作站、物理基础设施。
- **高级资源**　服务器、磁盘阵列、工作站群、人力资源。

3．制订通告计划

灾难发生时应及时向相关管理人员进行通报，不同级别的事件告知的形式是不一样

的。具体的形式见表 12-1。

表 12-1　不同级别事件告知形式

	低级别灾难	中级别灾难	高级别灾难
低级别资产	系统管理员	系统管理员	系统管理员，执法部门，企业管理员
中级别资产	系统管理员	系统管理员 企业管理员	系统管理员，执法部门，企业管理员

从表 12-1 中可以看出，不同级别的资产和不同级别的灾难环境下，所要告知的对象是不一样的。及时进行通报可以使管理员有时间采取相应的行为，减少灾难对信息系统的影响。

4．员工培训

由于灾难处理进程贯穿在整个企业的生命周期之中，因此对员工进行灾难处理培训是必要的。对不同的员工数量，其培训的方式也是不同的。

如果培训仅限于灾难恢复委员会范围中，则可以用研讨会的形式进行培训。如果培训范围在所有员工之中，则需要指派专人进行一次具体的宣讲。

12.5　使系统时刻处于准备之中

具体详尽的灾难恢复对于组织安全的作用十分重大，可以在灾难发生时尽可能减少损害。然而，随着组织情况的不断变化，不可能存在一个一成不变足以应对所有灾难的灾难恢复计划。灾难恢复计划需要实时贯穿在系统生命周期之中，也就是说灾难恢复计划要不断变化以适应新技术的发展。

1．时刻准备着应付灾难

灾难具有突发性，灾难真正发生的时候每一人都没有时间学习处理灾难的技巧，因此就应该提前做好准备工作。

（1）定期检测备份文件和恢复机制，确认能够从各种灾难中恢复需要的资料，确认所有的程序都被清晰定义，保证恢复机制能够有效率地执行。

（2）定期检阅系统日志和数据交换日志，保证在某些数据丢失时能有效地进行追溯。

2．时刻备份介质数据

对于灾难处理，最好的方式是备份。另外，还有一些操作是必须的，具体如下。

（1）建立定期检测已备份文件时间表并严格执行。

（2）进行文件的异地存储备份。

（3）建立表格表明需要备份的数据种类、备份地点以及备份时间。

3．风险评估

重要信息系统的灾难备份分析应包括对数据处理中心的风险分析、主要业务分析及

确定灾难恢复的目标等。

（1）数据处理中心风险分析

- 分析数据处理中心的风险，如物理安全、人为因素、已有的备份和恢复系统、基础设施脆弱点、数据处理中心位置、关键技术点等。
- 明确防范风险的技术与管理手段。
- 确定需要采取灾难恢复的类型，如灾难备份中心的距离、数据备份方式和频率等。

（2）业务分析

- 分析各项业务停业将造成的损失。
- 分析每项业务停顿的最大容忍时间。
- 分析各项业务的恢复优先级。
- 分析各项业务的相关性。
- 分析可接受的交易丢失程度。

（3）确定灾难恢复目标

- 确定恢复业务品种范围及优先级。
- 确定灾难备份中心及服务界面的恢复时限。

建立一个矩阵，行头包含所有可能发生的灾难类型，列头包含系统内所有有价值的资源，矩阵中每一个单元对应的是灾难对相应的资源所存在的潜在风险，这个矩阵一般由灾难管理委员会建立。

4．制订灾难备份方案

一个完整的灾难备份方案应基于灾难备份需求分析所得出的各业务系统灾难恢复目标，主要包括数据备份方案、备份处理系统、灾难备份中心建设、规程与管理制度。灾难备份方案一般分为 7 个级别：0 级（无异地异地备份）、1 级（实现异地备份）、2 级（热备份站点备份）、3 级（在线数据恢复）、4 级（定时数据备份）、5 级（实时数据备份）、6 级（零数据丢失）。具体内容见表 12-2。

表 12-2　灾难备份方案 7 个等级的比较表

级别	特点	适用场合
0 级：无异地备份	仅在本地备份，没制订灾难恢复计划，不具备真正灾难恢复能力，成本最低	是所有容灾方案的基础，从个人用户到企业级用户都广泛采用
1 级：实现异地备份	将关键数据备份到本地，后送异地保存，但异地无可用的备份中心	作为异地容灾的手段，此方案在许多中小网站和中小企业中采用较多
2 级：热备份站点备份	备份关键数据并存放到异地，制订相应的灾难恢复计划，备份介质采用交通运输方法送往异地，在异地有热备份中心，但保存的数据是上次备份的数据	灾难发生后可能会有几天甚至几周有数据丢失，故不能用于关键数据的容灾
3 级：在线数据恢复	通过网络将关键数据备份并存放到外地，制订相应的灾难恢复计划，有热备份中心	备份站点要保持持续运行，对网络要求较高，成本有所增加
4 级：定时数据备份	在 3 级方案基础上，用备份管理软件自动通过网络将部分关键数据定时备份到异地，并制订相应的灾难恢复计划	对备份管理软件和网络要求较高，导致成本增加，尚不能满足关键行业对关键数据容灾的要求

续表

级别	特点	适用场合
5 级：实时数据备份	在前几级容灾方案的基础上使用硬件镜像技术和软件的数据复制技术，关键应用使用双重在线存储，减少了数据的丢失量，降低了业务的恢复时间	既能保证当前交易正常进行，又能实时复制交易的数据到异地，是目前应用最广泛的方案
6 级：零数据丢失	利用专用网络将关键数据同步镜像到备份中心，数据在本地和异地都要进行确认，恢复速度最快， 实现零数据丢失	投资大，适合资金实力雄厚的大型企业和电信企业，适合交易较少或非实时交易的关键数据系统，目前采用此方案的用户不多

12.6 灾难备份技术

12.6.1 灾难备份中心

企业最为宝贵的财富就是数据，大量有关生产、销售、服务、管理的业务信息数据是企业珍贵无比、生死攸关的关键资产，它维系着整个公司和企业的生存发展。由于灾难无法避免，由灾难引起的数据丢失，对所有的企业组织来说无疑是一场灾难。这种灾难除了给企业带来巨大的经济损失，甚至有可能动摇企业的生存基础。据调查显示，只有 6%的公司，企业可以在数据丢失之后生存下来，43%的公司会彻底关闭。 可见企业享受因为信息化带来的快捷的服务和方便的管理时，也必须面对数据丢失的风险，容灾是确保信息安全的一个关键策略。如何确保数据信息系统在最短的时间内恢复是企业面临的最大挑战。

灾难备份中心是为了确保重要信息系统的数据安全和关键业务可以持续服务，提高抵御灾难的能力，减少灾难造成的损失而建设的数据备份系统。灾难备份系统是整个信息系统的有机组成部分，而不是游离于生产系统之外的一个独立系统，更不是一个可有可无的东西。数据灾难备份服务起源于 20 世纪 70 年代，目前在发达国家已成为信息工业中增长最快的行业之一。

目前，灾难备份的主要行业应用是：在政府或企业的信息数据中心遭遇自然灾难或人为侵害时，启用同城或异地建立的备份数据中心提供不间断的数据信息服务，从而保证政府或企业的业务连续性。在政府、金融、电信、交通、能源、公共服务业及大型制造及零售业等信息化依存程度高的行业，灾难备份应用极其广泛。

目前灾难备份中心的建设模式有以下 3 种：①自建灾难备份中心模式；②共建灾难备份中心模式；③服务外包模式。

12.6.2 灾难备份与恢复技术

真正的灾难备份必须满足以下三大要素：①冗余性（Redundance），即系统中的部件、数据都应该具备冗余性，当某个系统发生故障时，另一个系统能够确保数据传送的顺畅性；②长距离性（Remote），由于灾害总是发生在一定范围内，因而保持足够长的距离

才能保证数据不会被同一个灾害全部毁坏；③可复制性（Replication），灾难备份系统追求全方位的数据复制。

灾难备份的目的是确保灾难发生后业务立即恢复，应用能够尽快投入使用，采用的各种技术不论是数据备份、数据复制还是灾难备份技术，都是围绕着业务的连续性来进行，这些技术是灾难备份的关键环节。而衡量这些技术标准就是 RPO（Recovery Point Object，恢复点目标）和 RTO（Recovery Time Object，恢复时间目标），也就是出现灾难的时候多长时间可以让业务继续运作，同时会丢失多长时间的数据。具体采用哪项技术，完全要根据实际需求，再结合各种技术能够达到的 RTO 和 RPO 指标来决定，需要说明的是，追求两个技术指标都是零的做法是不经济的，也是不现实的，任何事情都要考虑投入产出比和回报。

一个完整的灾难备份系统主要由数据备份系统、备份数据处理系统、备份通信网络系统和完善的灾难恢复计划构成。其中，数据备份是整个系统的关键，如何将系统数据、应用数据和业务数据等完整、实时地复制到灾难备份中心，是整个灾难备份系统首先要重点考虑到的。目前，比较流行的数据实时复制技术主要有两种：数据备份技术和数据存储备份技术。典型的灾难备份系统如图 12-1 所示。

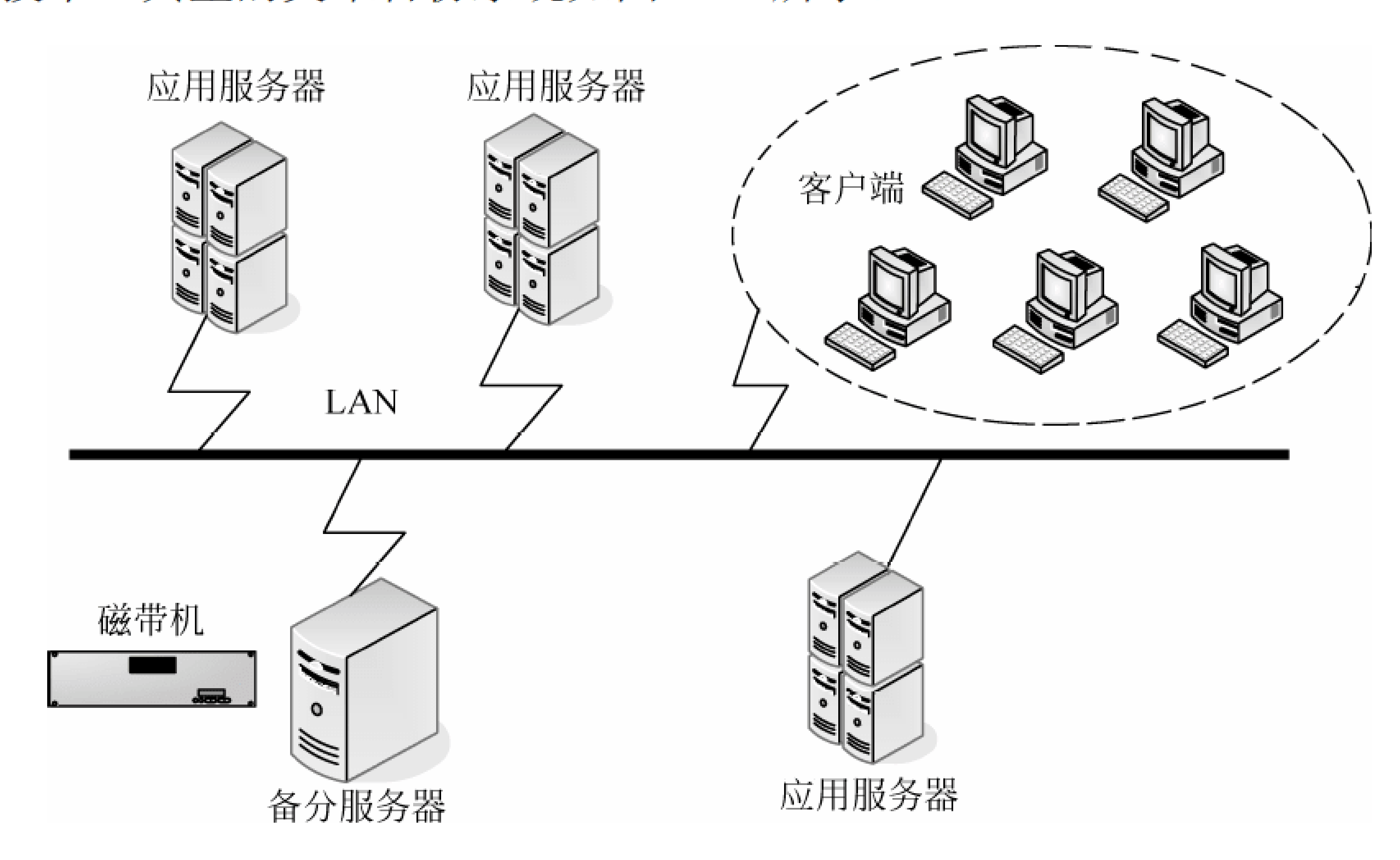


图 12-1　典型的灾难备份系统

12.6.3　数据备份技术

数据备份技术主要包括基于磁盘系统的灾难备份技术、基于软件方式的灾难备份技术和其他灾难备份技术的解决方案 3 类。

1．基于磁盘系统的灾难备份技术

基于磁盘系统的远程数据备份技术是以磁盘系统为基础，采用硬件数据复制技术，借助磁盘控制器提供的功能，通过专线实现物理存储器之间的数据交换。这种方式的优点是，它独立于主机和主机操作系统，不占用主机的 CPU、主机通道和网络资源，对主

机透明，也不需要对现有应用系统做任何改动。

基于磁盘系统的灾难备份技术可采用以下两种方式工作：同步数据复制模式和异步数据复制模式，见表 12-3。

表 12-3 基于磁盘系统的灾难备份技术工作方式

工作方式	技术特点	优缺点
同步数据复制模式	来自处理器的更新数据在写入本地连接的磁盘系统之前，通过磁盘镜像技术，将更新数据转发至异地的磁盘系统，只有更新数据在两个磁盘系统完成写操作后，本地磁盘系统才会向处理器返回写完成指令，从而保证了两地磁盘系统数据的一致性和完整性，即无数据丢失	优点：远端数据与本地数据的实时性强，灾难发生时远端数据与本地数据完全同步 缺点：本地的交易受网络的影响较大，应用系统将会因等待 I/O 写操作而被延迟，致使本地的 I/O 访问效率下降，另外，此模式的数据传输距离较短（一般专线距离在 60 千米以内）
异步数据复制模式	来自处理器的更新数据首先被写入本地连接的磁盘系统，并立即向处理器返回一个 I/O 写完成指令，之后磁盘镜像系统在很短的时间内，将更新数据发送至异地的磁盘系统。该模式在软件灾难备份技术中广泛使用，而硬件灾难备份技术一般不采用	优点：对应用程序的运行性能影响较小，不影响本地的交易，传输距离可长达 1000 千米以上，受远程网络的影响较小 缺点：远程磁盘系统的数据比本地磁盘系统的数据略有一个时间延迟，若远程网络带宽较小，网络阻塞较大

2．基于软件方式的灾难备份技术

软件方式的灾难备份技术是基于操作系统级的灾难备份解决方案。其特点是与操作系统平台相关，而对应用程序是透明的。此方式通过通信网络，实现数据在两个不同地点之间的实时备份。

3．其他灾难备份技术的解决方案

目前，各大知名数据业务公司都相继推出自己的灾难备份技术解决方案，如通过磁带库技术实现数据远程备份解决方案，Sybase、Oracle 的数据库镜像技术解决方案等。

12.6.4 数据的存储技术

灾难备份的另一项关键技术是数据的存储备份技术。其中，提高灾难备份系统性能最重要的指标就是存储优化。目前，常用的存储优化技术有 DAS（Direct Attached Storage，直接连接存储）、NAS（Network Attached Storage，网络连接存储）和 SAN（Storage Area Network，存储区域网络）。

1．DAS 存储结构

DAS 是最早用于网络的存储系统，它以服务器为中心。如图 12-2 所示，在 DAS 中，数据被存储在各服务器的磁盘族或磁盘阵列等存储设备中。

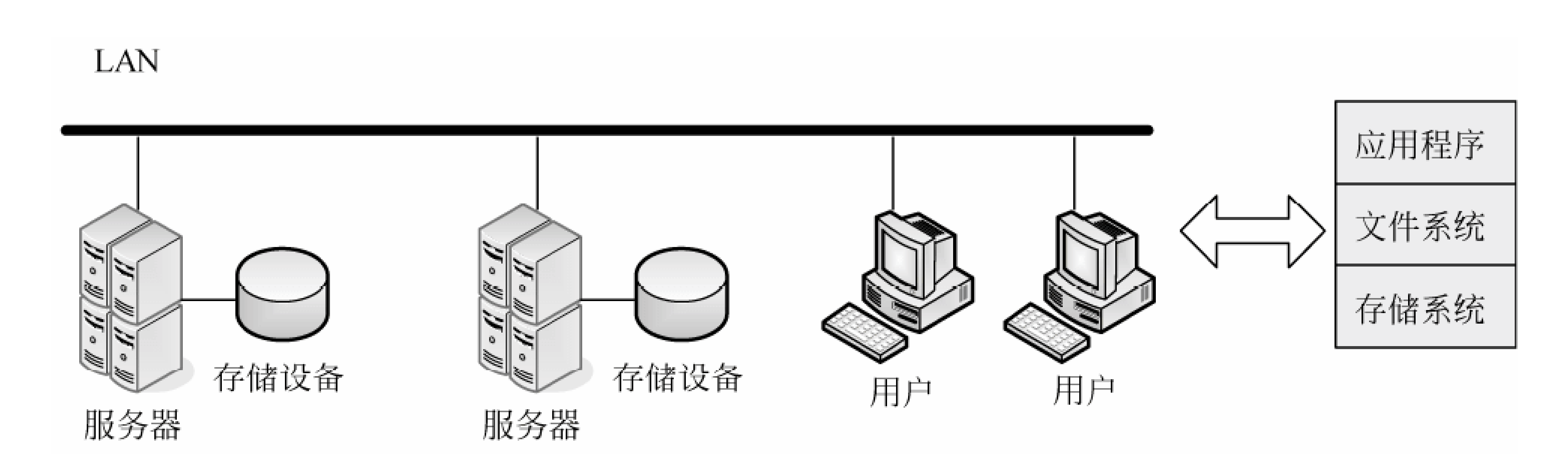


图 12-2　DAS 的存储结构

DAS 依赖服务器主机操作系统进行数据的 IO 读写和存储维护管理，数据备份和恢复要求占用服务器主机资源（包括 CPU、系统 IO 等），数据流需要回流主机再到服务器连接着的磁带机（库），数据备份通常占用服务器主机资源的 20%～30%，因此为了避免影响正常业务系统的运行，许多企业用户通常在夜间或业务系统不繁忙时进行日常数据的备份。

DAS 与服务器主机之间通常采用 SCSI 连接，带宽一般为 10MB/s、20MB/s、40MB/s、80MB/s 等，随着服务器中央处理器的处理能力越来越高，存储硬盘空间越来越大，阵列的磁盘数量越来越多，SCSI 通道将会成为 IO 瓶颈。

DAS 的数据量越大，备份和恢复的时间就越长，对服务器硬件的依赖性和影响就越大。其优点是存取速度快、建立方便；但也存在一些明显的缺点，如单点错误问题、扩展困难等。

（1）单点错误问题

即当网络上某一设备出故障时，这将导致整个网络都将无法正常工作。解决方案是使多个服务器共享一个存储系统，形成如图 12-3 所示的直接连接共享存储系统。

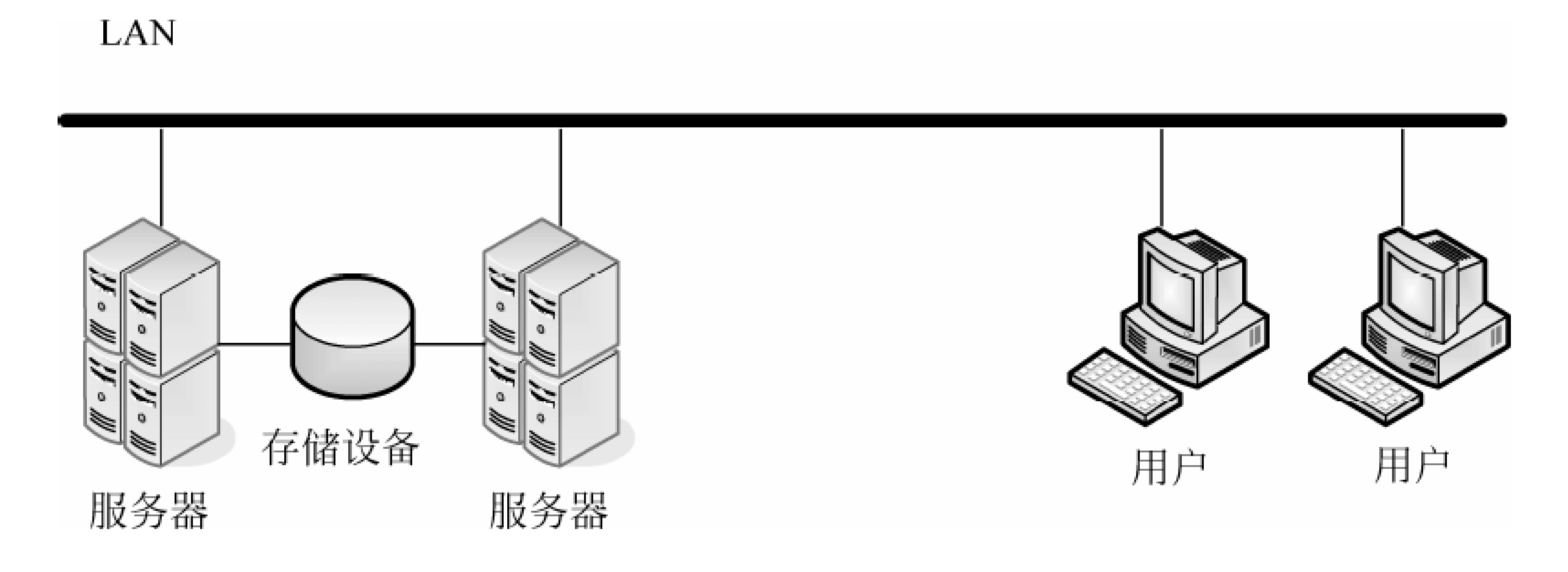


图 12-3　直接连接的共享式存储系统的存储结构

（2）扩展困难

虽然可以通过添加设备的方式增大存储容量，但因各种计算机外部设备都连接在通用服务器上，而标准计算机可连接的存储设备的接口有限，添加设备也需要较高的费用；此外，因添加设备后会出现所有服务器都试图访问存储设备的情况，势必造成网络拥塞，降低了其可靠性、安全性和稳定性。

因此，DAS 的存储结构有明显的局限性，它适合小型企业，而不适合大企业数据吞

吐量较大、并发用户数量较多的需求。

2. NAS 存储结构

如图 12-4 所示，NAS 是一种采用直接与网络介质相连的特殊设备实现数据存储的机制，它以数据为中心，将存储设备与服务器彻底分离（数据的存储与处理功能分离），服务器只用于处理数据，而文件服务器只用于存储数据。这就是 NAS 存储系统的特点，其开发目的是在不消耗大量网络带宽的情况下实现存储功能，这种存储结构可完全脱离服务器就能直接上网。NAS 本身能够支持多种协议（如 NFS、CIFS、FTP、HTTP 等），而且能够支持各种操作系统。通过任何一台工作站，采用 IE 或 Netscape 浏览器就可以对 NAS 设备进行直观方便的管理。

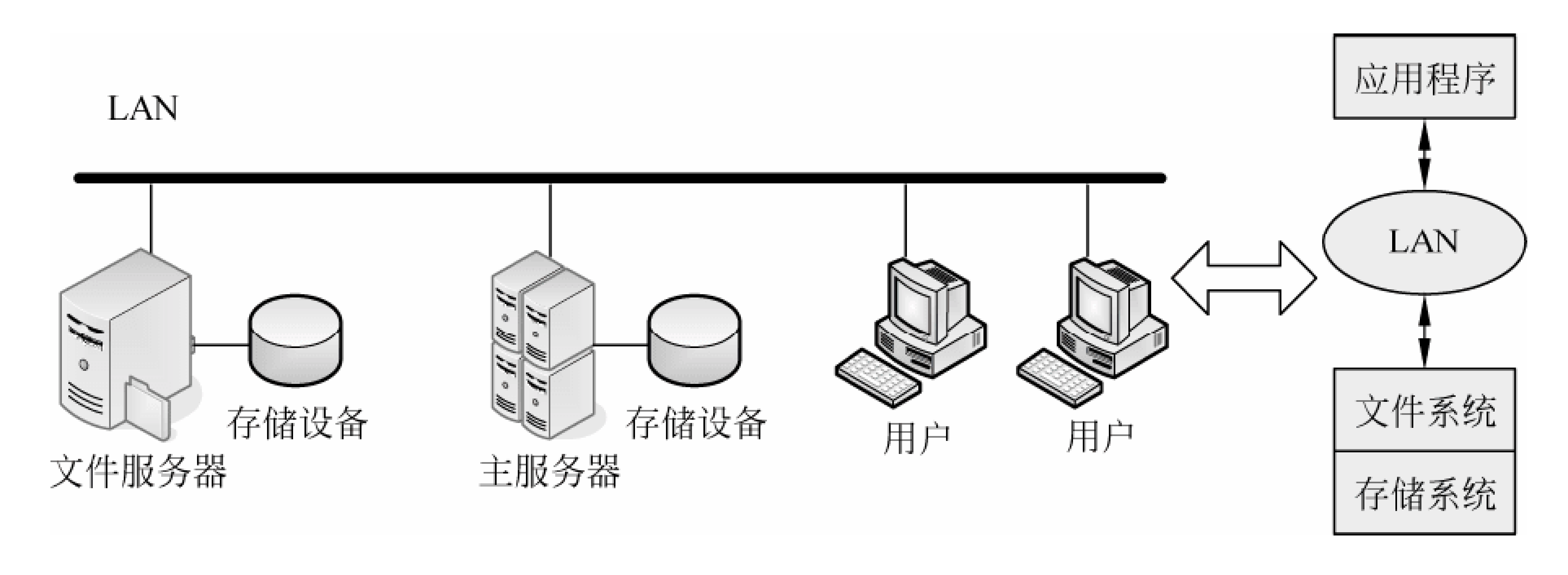


图 12-4　NAS 的存储结构

NAS 存储系统有很多优点，主要表现在以下几个方面。

（1）数据存储和数据处理功能分离，消除了网络的带宽瓶颈。当网络服务器崩溃时，用户仍能访问 NAS 设备中的数据；当 NAS 故障时，网络上与主服务器相关的其他操作也不会受到影响，甚至更新或替换存储设备时也不需关闭整个网络。

（2）NAS 设备不依赖于通用的操作系统，而是采用了瘦服务器（Thin Server）技术，应用于高效的文件共享任务中，不同的主机与客户端通过文件共享协定存取 NAS 上的数据，实现文件共享功能。例如 UNIX 中的 NFS 和 Windows NT 中的 CIFS，其中基于网络的文件级锁定提供了高级并发访问保护的功能。

（3）实现简单。NAS 存储结构成本较低、易于安装、管理和扩展、使用性能和可靠性均较高，适用于那些需要通过网络将文件数据传送到多台客户机上的用户。NAS 设备在数据必须长距离传送的环境中可以很好地发挥作用。

3. SAN 存储结构

当 DAS 和 NAS 在访问存储设备时，必须经过 LAN。在 LAN 中，不仅要由 LAN 连接多台服务器和大量客户机端的设备、还要连接存储设备、协调客户机/服务器的数据。此外，随着备份数据和数据复制需求的大幅增长，连接服务器与存储设备的 SCSI（Small Computer System Interface）接口由于受距离、连接端口数和带宽的限制，容易因超载而产生瓶颈。

图 12-5 是 SAN 的结构示意图。SAN 是一种专用高速网络或子网络，用于连接服务

器和存储装置（大容量磁盘阵列和备份磁带库），提供在计算机与存储系统之间的数据传输。这种连接是基于固有的 FC 通道（Fiber Channel，光纤通道）和 SCSI 技术，通过 SCSI 到 FC 通道转换器和网关，一个或多个 FC 通道交换机在主服务器与存储设备之间提供相互联接，形成一种特殊的高速网络。一个 SAN 网络由负责网络连接的通信结构、负责组织连接的管理层、存储部件以及计算机系统构成，从而保证数据传输的安全性和力度。可以把 SAN 看成是 LAN 之下的第二网络，它不涉及 LAN 的具体操作。

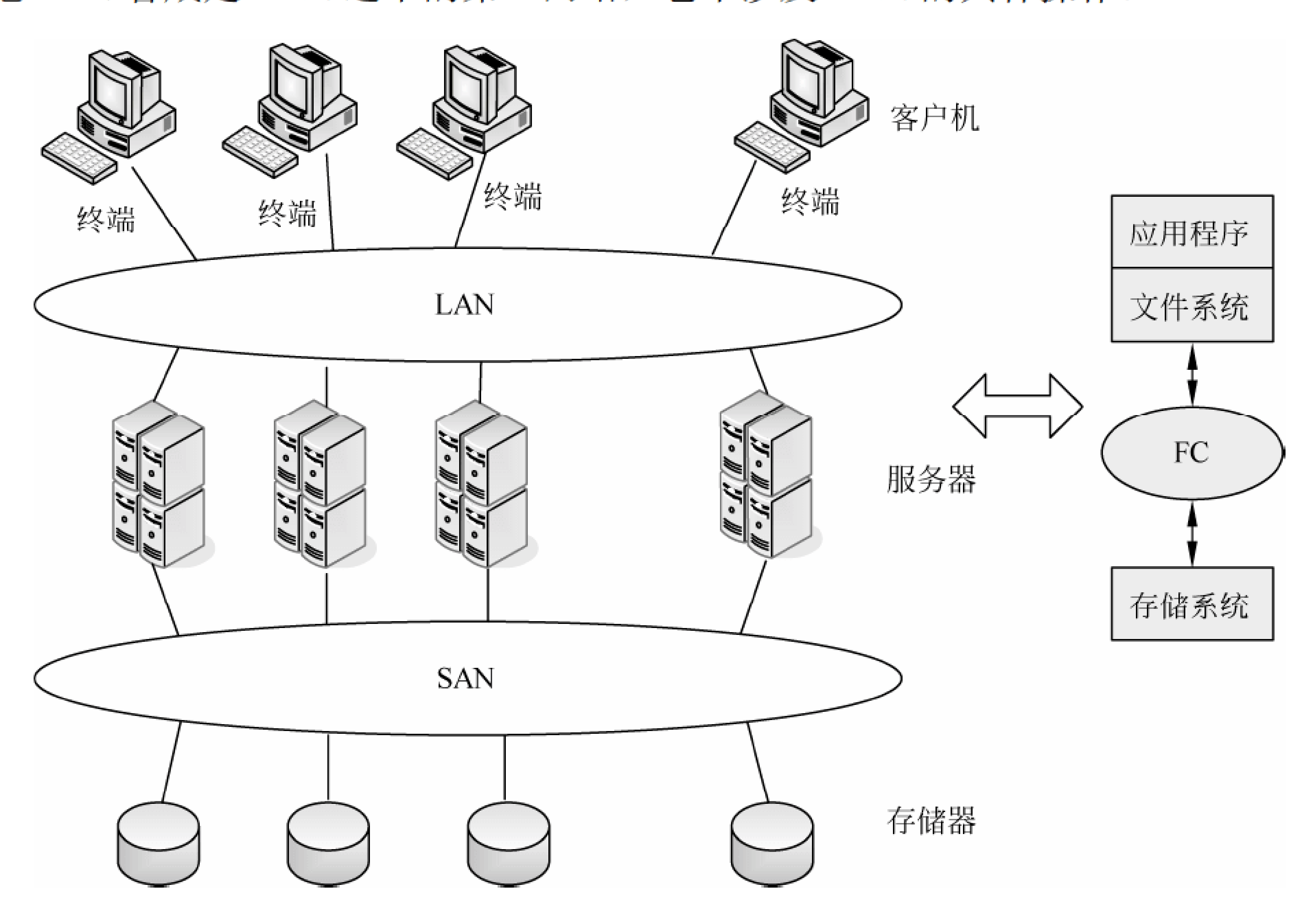


图 12-5 SAN 的结构

SAN 具有如下优点。

（1）使用 FC 通道调节技术来优化存储器与服务器之间的数据快传输，通过支持存储器与服务器之间进行大容量数据块传递软件，减少了发送对数据块的分割，也减少了对通信节点的预处理，从而具有更快的响应速度和更高的数据带宽。

（2）高性能的 FC 交换机和 FC 网络的使用确保了设备连接的可靠性和高效率，提高了容错度。

（3）利用多条 FC 链路建立冗余通道，保证了传输链路的可靠性，通过 SAN 内部的 FC 网络建立多层次的存储备份体系，保证了系统的高可靠性，这都保证了企业的数据完整性、可靠性和安全性要求。

（4）基于网络的存储虚拟化，将主机与存储的联系断开，可动态地从集中存储中分配存储量。虚拟存储的可伸缩性简化了网络服务的使用和可扩展性，也提高了硬件设备的初期回报。

（5）提供高效的故障恢复环境，大大提高了应用软件的可用性。

（6）安装容易、快速，对服务器的要求降低，可大大降低服务器的成本，有利于高性能存储系统在更广的范围内普及及应用。

4．SAN 与 DAS、NAS 的比较

从图 12-4 和图 12-5 右侧的比较中可看出，DAS 的应用程序与存储系统是一体的，通过系统总线可访问存储设备；传统的 NAS 是应用与存储分离的系统，应用服务器通过 LAN 访问文件存储系统，通常 NAS 以标准化协议（如 NFS）提供服务；在 SAN 中，文件系统与存储系统完全分离，存储系统实际上成为运行应用程序的数据服务器，两者以高速光纤通道 FC 连接，如图 12-6 所示。

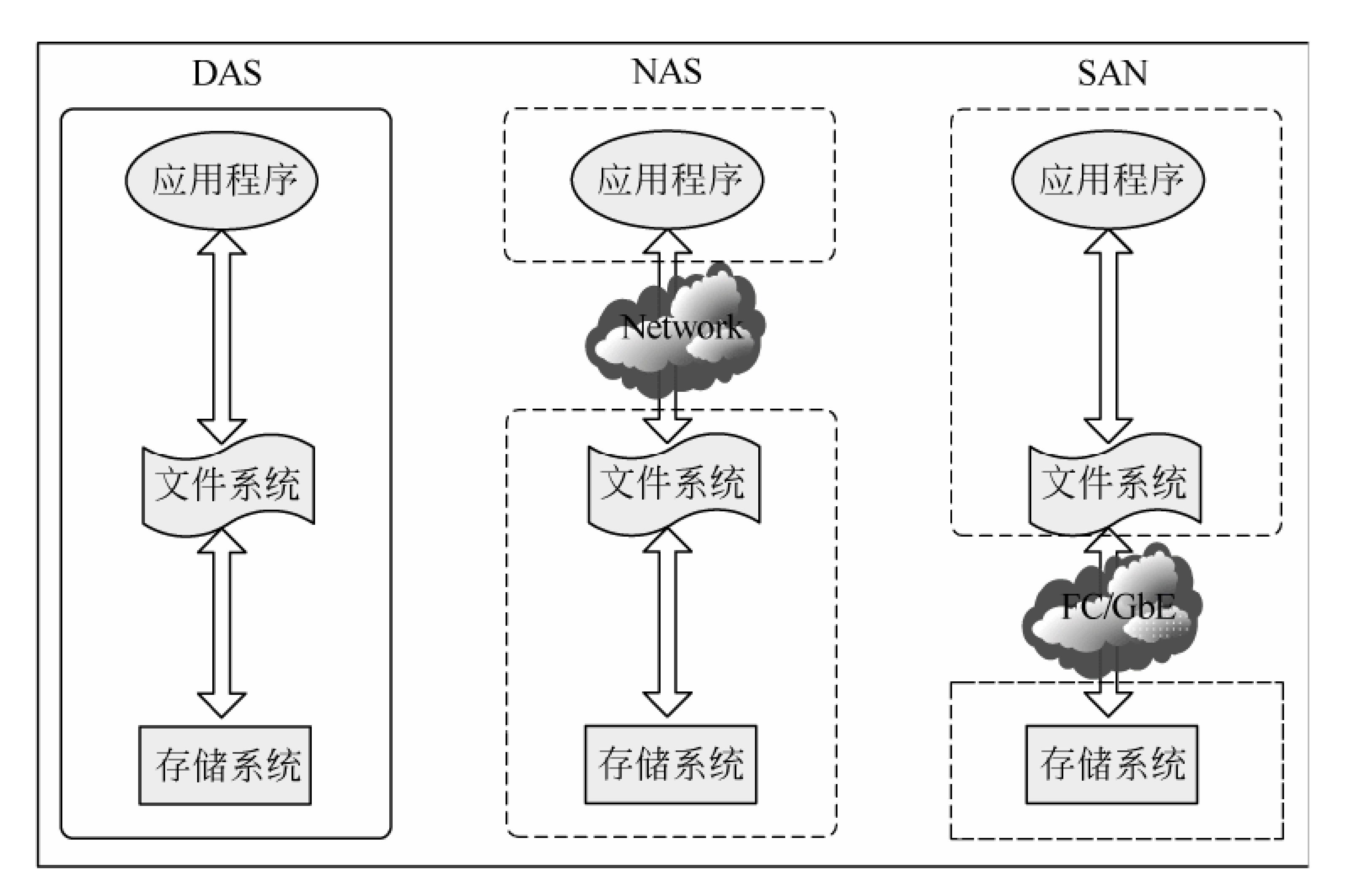


图 12-6　DAS、NAS 和 SAN 的比较

DAS、SAN 和 NAS 组织图如图 12-7 所示。

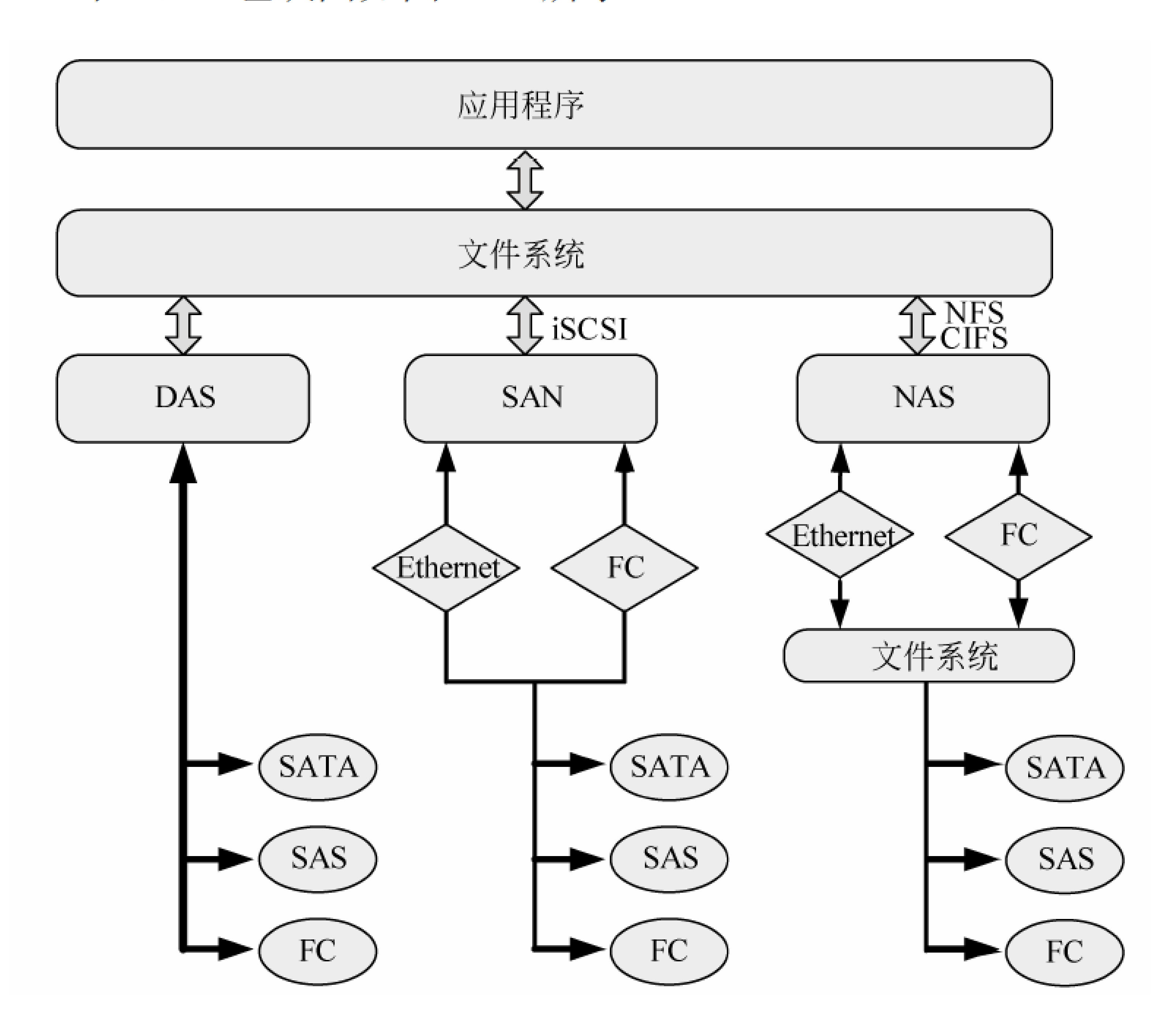


图 12-7　DAS、SAN、NAS 组织图

NAS 允许多台计算机经过网络访问同一个文件系统，并且会自动同步它们的操作。由于 NAS head 的引入使得 SAN 存储可以容易地转换为 NAS。尽管 NAS 和 SAN 有所区别，但还是有方法可以提供两项技术均被包括在内的混合应用解决方案。图 12-8 描述了使用了 DAS、NAS 和 SAN 技术的混合解决方案。

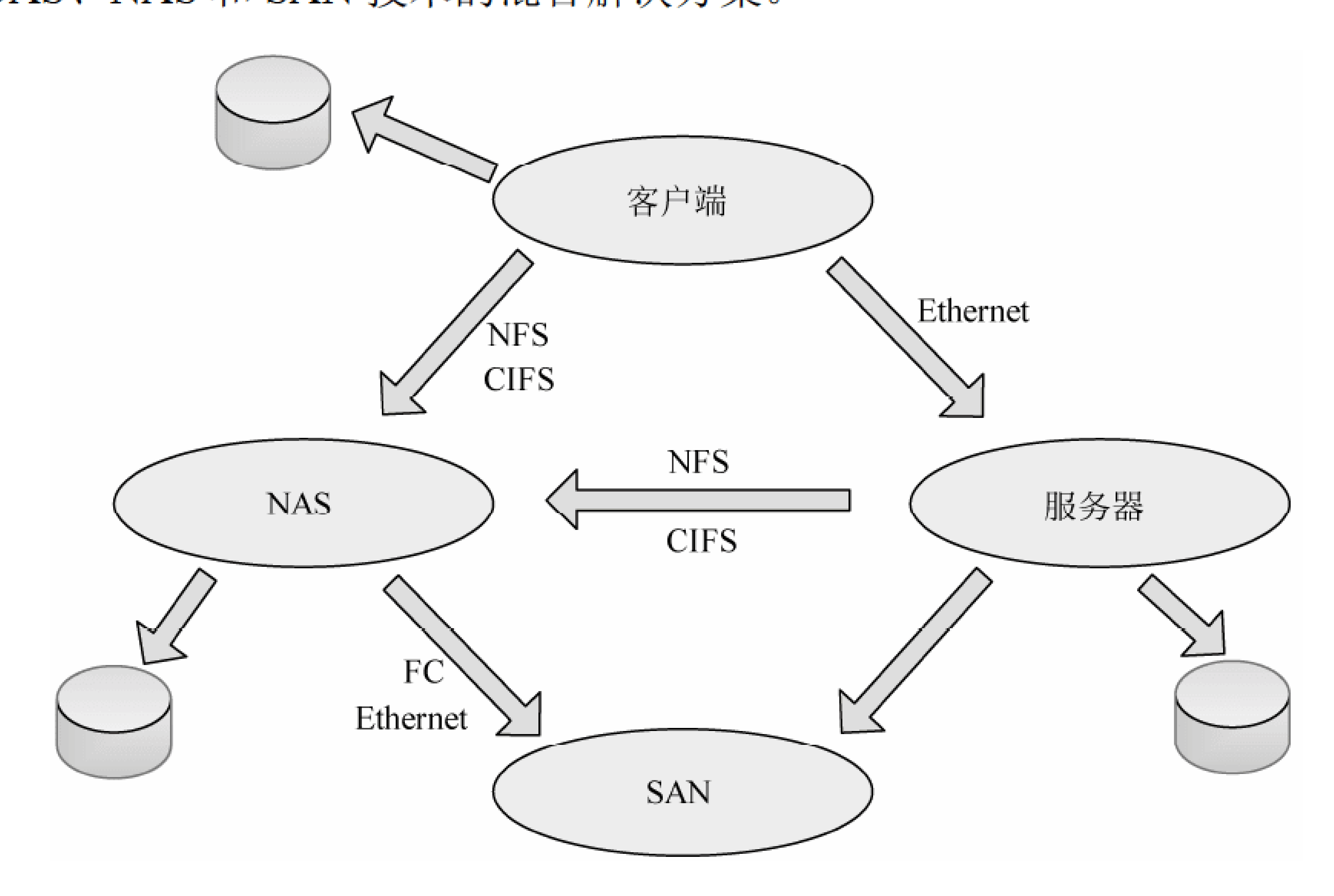


图 12-8　使用了 DAS、NAS 和 SAN 技术的混合解决方案

典型的 SAN 是一个企业整个计算机网络资源的一部分，它支持磁盘镜像技术、备份与恢复、档案数据的存档和检索、存储设备间的数据迁移以及网络中不同服务器间的数据共享等功能，通常与其他计算资源紧密结合来实现远程备份和档案存储过程。

综上所述，SAN 和 NAS 是当今两种主流的网络存储技术，它们克服了传统存储技术的缺点，必将占有未来存储系统的主导地位。

12.6.5　CDP 连续数据保护技术

1. CDP 连续数据保护技术的概念

CDP（Continuous Data Protection，持续数据保护）技术是目前最热门的数据保护技术，是对传统数据备份技术的一次革命性的重大突破。传统的数据备份解决方案专注在对数据的周期性备份上，因此一直伴随有备份窗口、数据一致性以及对生产系统的影响等问题。现在，CDP 为用户提供了新的数据保护手段，CDP 系统会不断监测关键数据的变化，不断地自动实现数据的保护系统，管理员无须关注数据的备份过程，而是仅当灾难发生后，简单地选择需要恢复到的时间点即可实现数据的快速恢复。

CDP 技术可以捕捉到一切文件级或数据块级别的数据写改动，可以对备份对象进行更加细化的粒度的恢复，可以恢复到任意时间点，通过在操作系统核心层中植入文件过滤驱动程序来实时捕获所有文件访问操作。对于需要 CDP 连续备份保护的文件，当 CDP

管理模块经由文件过滤驱动拦截到其改写操作时，则预先将文件数据变化部分连同当前的系统时间戳一起自动备份到 UnaCDP 存储体。从理论上说，任何一次的文件数据变化都会被自动记录，因而称之为持续数据保护。

2. CDP 与传统备份技术的对比

传统的备份技术一般为手动备份或定时备份，效果非常有限。典型的手动备份流程是：每日凌晨进行一次增量备份，然后每周末凌晨进行全备份。采用这种方法，一旦出现了数据灾难，用户可以恢复到某一天的数据，因此在最坏的情况下，可能丢失整整一天的数据。定时备份技术比手动备份技术先进了不少，它属于自动备份的技术范畴，通常为若干小时自动备份一次，比如：每 6 小时备份一次。如果数据灾难发生了，用户可以恢复到若干小时之前的数据，在最坏的情况下，可能丢失 6 小时内的数据。但是对于数据量不断变化增长的用户来说，每一份数据的丢失都会造成巨大的利益损失。

于是，用户就希望能继续缩小备份时间单位，如每小时甚至每分钟备份一次。传统的备份技术对这个问题是无能为力的，而 CDP 正是为了解决这个问题而出现的，它能做到连续的数据保护。

CDP 技术是一种连续捕获和保存数据变化，并将变化后的数据独立于初始数据进行保存的方法，而且该方法可以实现过去任意一个时间点的数据恢复。CDP 系统可能基于块、文件或应用，并且为数量无限的可变恢复点提供精细的可恢复对象。因此，所有的 CDP 解决方案都应当具备以下几个基本的特性。

（1）数据的改变受到连续的捕获和跟踪。

（2）所有的数据改变都存储在一个与主存储地点不同的独立地点中。

（3）恢复点目标是任意的，而且不需要在实际恢复之前事先定义。

所以，CDP 技术可以提供更快的数据检索、更强的数据保护和更高的业务连续性能力，而与传统的备份解决方案相比，CDP 的总体成本和复杂性都要低。

3. CDP 技术分类

CDP 技术的分类是相对于数据保护时间点而已的，它分为准 CDP 和真 CDP 两种。

（1）准 CDP

准 CDP（Near CDP）技术是按照一定的时间频率持续地记录并备份数据变化，每次备份有一定时间窗口，需要数据恢复时，可以恢复到过去备份的时间点，并不能形成完全意义上的持续保护。它的最大特点是只能恢复部分指定时间点的数据（Fixed Point In Time，FPIT），有点类似于存储系统的逻辑快照，它无法恢复任意一个时间点。目前 Symantec、CommVault 的 CDP 都属于这种类型。

（2）真 CDP

真 CDP（True CDP）技术是持续不间断地监控并备份数据变化，可以恢复到过去任意时间点（Any Point In Time，APIT），是真正的实时备份。目前 BakBone TrueCDP 属于真 CDP 类型。

习　题

一、选择题

1．下列哪一项不属于发生在本地的中级别灾难？（　　）

A．病毒攻击

B．长时间的停电

C．服务出错

D．服务器故障

2．以下哪一项不属于系统灾难恢复的准备工作？（　　）

A．Internet 信息服务

B．风险评估

C．备份介质数据

D．应付灾难准备

二、简答题

1．简述制订灾难恢复计划的过程。

2．制订通告计划的作用是什么？

3. 灾难备份都有哪些技术，其原理是什么？

4．当前都有哪些数据存储技术，其优缺点是什么？

5．简述 CDP 连续数据保护技术。

6．对灾难备份方案的 7 个等级，从每个等级的特点和适用场合进行比较。

课后实践与思考

1．描述您所在的单位/组织的灾难备份中心是如何运作的。

2. 了解您所在的单位/组织是如何对员工进行有关灾难备份的培训的，其效果如何？

第 13 章　计算机与网络取证技术

本章学习重点：

- 理解计算机取证的含义
- 学习计算机取证的技术及其过程
- 认识计算机证据分析方法
- 学习如何进行网络取证
- 使用取证工具

随着计算机技术的发展，很多网络技术的成本骤然下降。计算设备与通信设备的小型化，以及全球化的影响，计算机技术对社会的影响会越来越高。同时犯罪分子也会更容易运用计算机进行犯罪。基于上述背景，计算机取证技术应运而生。

13.1　基本概念

计算机取证是以计算机为基础的司法鉴定科学技术。通过以计算机为基础的资料作为证据，涉及提取、审查、保存、分析、评价，从而为民事、刑事、行政和其他案件提供有关的信息。简单来说，计算机取证技术就是在计算机的存储介质，如硬盘或其他磁盘中，进行信息检索和调查。

不同于计算机取证，网络取证是从网络存储设备中获取信息，也就是从网络上开放的端口中检索信息来进行调查。很多时候，网络取证比计算机取证要麻烦，当面对 2 台或 3 台计算机时，对其进行拍照取证是很简单的，而当在网络中面对数千个网络节点时，这几乎是不可能的。

计算机犯罪侦查与网络犯罪侦查是不一样的。计算机犯罪侦查的案件特点是以计算机为工具或以计算机为目标的案件，计算机在犯罪过程中扮演了很重要的角色，所有侦查的重点都围绕计算机而开展，所有与案件有关的信息都可以由计算机的固定硬盘和移动硬盘中提取出来或推断出来。

虽然网络取证是源于计算机取证，并且两者的目的都是一样——破获案件，但网络取证还是有自己的特点，主要表现在以下两个方面。

（1）在计算机侦查中，侦查员和罪犯对系统的了解程度是不一样的，一般来说侦查员相对于罪犯更加了解目标系统，而网络侦查中，双方对系统的理解程度是一样的。

（2）在网络取证的很多情况下，侦查员与罪犯使用的是同种工具。如今市场上有一些获取系统信息的安全工具，有些人将其用于获取线索，而有些人就将其用于非法牟利。

13.2 计算机取证技术

13.2.1 计算机取证基本元素

犯罪侦查中有 3 个核心的元素：线索材料、与案件有关的材料、案件材料的合法性。由于计算机取证与传统取证非常类似，因此计算机取证中也存在这几个元素。

1. 线索材料

计算机犯罪中涉及的材料包括物理的和电子的材料。物理材料属于传统警方的范围，例如对文件、信封、箱子等进行检查。而电子材料就相对复杂一点，其有可能是存放在硬盘中的数据、电子邮件的内容、电子邮件的地址、附件和网站日志文件等；也有可能是已经删除掉的文件（计算机中文件删除后是可以恢复的），因为常用的删除操作只是将其从计算机的目录中删除，而实际数据还是存放在硬盘中；还有一种数据就是加密数据，获取这种数据信息的难度相对要高一些。

如果计算机是调查对象的话，那么计算机所有组件的信息都是要被搜查的对象，例如系统在操作过程中会产生很多管理信息、控制信息等，这些对日后的侦查都可能起着决定性的作用。

2. 相关信息

收集到上述信息后，下一步就是要确定哪些信息与案件相关。材料的相关性取决于委托人、要求的内容和调查的安全类型。代理一般有受害人、政府、保险公司、法院、执法部门等。

3. 合法性

数据的合法性问题与数据的关联性问题是一致的，其同样基于数据的认证过程。

13.2.2 计算机取证过程

计算机取证和网络取证的过程是一样的，分为 3 个步骤：①寻找证据；②保存证据并确保其完整性不受损坏；③对提取出来的数据进行合法性认证，具体包括确认数据是原始数据而没有经过修改。

1. 寻找证据

处理计算机案件时，必须要认清收集证据的困难程度。一般证据分为以下几类。

- **痕迹** 包括指纹、刀痕、鞋印或其他遗留下来的痕迹。
- **生物痕迹** 包括血迹、毛发、指甲壳、汗液等。
- **信息痕迹** 保存在存储设备中的二进制数据等。

当信息收集完以后，侦查员就要开始创建罪犯的轮廓。这时，就应该让嫌疑系统运转一段时间，这样有助于证据的收集。值得注意的是需要提前做好系统的复本，实际上运行的系统为原系统的复本，而原系统处于停止运行的状态，这样做是为了防止原系统的一些数据证据由于程序的运行而被修改或者删除。但这样做的同时也会有些缺点，例如可能会导致某些正在运行的程序数据的丢失。

在对系统进行数据取证的时候，要慎用一些工具软件。在使用前要对软件的优势与劣势进行分析。很多调查员选择不在系统上使用任何软件，防止原来运行的软件受损。不过在原系统的复本系统里面，可以使用这些侦查软件。

2. 处理证据

证据的合法性源于证据的完整性，案件最终的成功与否与侦查时所取得的证据有很大关系，与证据是否切合案件事实有很大关系。所以在处理证据的时候，需要格外地小心。证据处理包括证据提取和证据保管，证据保管包括包装、存储和运输。在处理这几个环节时，要注意以下问题，便于日后审查。

（1）证据提取负责人及提取方法。

（2）证据包装负责人。

（3）证据保管负责人、保管方式以及保管位置。

（4）证据运输负责人。

3. 证据恢复

提取证据时要尽可能将所有的证据都收集到，避免重回现场取证。具体来说需要检查的资料涉及计算机硬件、软件、文档等内容，硬件方面包括计算机、打印机、扫描仪和一些网络连接设备；软件方面包括系统软件、系统日志、应用程序软件和用户具体使用的软件；文档方面包括现场打印出来的材料和碎纸机里面的纸屑等；同时要留意录音带、移动硬盘等移动存储设备。

证据提取方式取决于采集数据的大小、采集数据的时间和保存数据的时间。对大容量硬盘中的证据，有必要在提取时使用压缩和复制的方式。一般压缩方式有两种：无损压缩和有损压缩。在计算机取证中，无损压缩的工具一般为 WinZip 和 PKZip，压缩时常常使用 MD5、SHA-1 算法，或进行 CRC 校验从而保证压缩数据的安全性。

对于每个项目中提取的证据，要分配一个唯一的标识号，并在每一个项目上写出简短的介绍，如证据的提取地点、提取时间、提取负责人等。也可通过照相或摄影的方式来保持现场的证据，最好用摄像机将整个取证过程拍摄下来，这样就增加了一个现场证据。

当所有证据都被收集并分类整理之后，就要将其存放在一个安全的位置，来保证证据的完好无损。例如，该位置必须干燥干净，并且周围的磁性不能太强。还需要设置一个相同的复本保证证据的安全性。

取证时往往会碰到一些加密的证据，例如加密的电子邮件、数据文件和硬盘。侦查员可以借助各种工具来完成相应的解密工作，对于加密的电子邮件可以使用 PGP，对隐藏的加密文件可以使用 EMF、Crytext 和 Date Fortess，对硬盘加密可以使用

BestCrypt 等。

4．证据保存

目前还没有一个保护证据安全的标准方法。将证据封装并不能保证其完整性，可以采取其他存储措施长时间地存储证据。保存电子证据的困难之一是证据的易失性，在进行证据保存时，必须要考虑到这个因素。

保存证据需要注意以下方面因素。

（1）将证据封装并进行归类，然后放置于无静电环境下。确保封装后的证据不会被过冷、过热或过湿的环境所影响。

（2）将原始数据进行备份，对所有嫌疑存储介质做磁盘镜像。

（3）条件允许情况下，要对证据数据进行加密。加密可同时被侦查员和罪犯所用。作为罪犯，一般利用加密进行内容隐藏；作为侦查员，一般利用加密保证证据的保密性和完整性。

（4）存储证据时，要对证据执行可信的访问控制策略，以确保证据只能被授权人员使用。

5．证据传输

信息证据往往要进行多次传输，例如从犯罪现场传输到某个安全位置，或传到法院等。在传输过程中必须要保证证据完整性不被破坏，要注意防范数据传输过程中可能出现的陷阱。证据传输过程中，要注意以下几点。

（1）由于在传输过程中，可信的内部人员能够接触到证据，因此为保持监管，应该检查沿途所有处理过证据的人员的数字签名。

（2）在传输过程中，要使用一些强大的数据隐藏技术，例如数据加密、信息隐藏、密码保护等对证据进行保护。

（3）需要一些方法能够检测出信息证据在传输过程中是否出现过更改变动。一般来说，校验的方法有奇偶校验、冗余校验与校验和等方式。随着技术的进步，可以利用 Hash 函数对校验和进行加密来判断证据是否有过更改。被 Hash 函数进行加密的校验和叫做证据的消息摘要。Hash 函数主要有 MD5 和 SHA-1 散列算法，利用算法的不可逆性可以验证证据是否被修改。

13.2.3　计算机证据分析

对证据进行提取、标识、存储和传输之后，就要进行计算机和网络取证中最为重要最为耗时的环节——证据分析。在证据分析过程中，侦查员会对提取的数据进行分析来确认犯罪嫌疑人的行为模式、异常文件签名、异常行为等一系列和案件相关的线索。

当进行证据保管时，实际就是证据分析的开始。确保所有的证据都已被送往检验中心，所有的项目都被放在证据袋中。证据分析开始前，所有的证据认证工作应该都已经结束。对于每一个磁盘或其他记录媒体，必须要做一个镜像，目前常用的此类软件有 DeriveSpy、EnCase、CaptureIt 和 FTKExplorer。

硬盘处理结束后，下一步就是处理其他的外围设备、文件和其他所有与本案相关的组件。具体使用的工具将在下面几节介绍。选用不同的平台，会导致证据分析的工作量和分析的质量不同。

1. 隐藏的证据

进行证据分析时，侦查员会经常遇到一些不能直接读取、隐藏于系统中的数据，而这些数据往往隐藏了关于案件的重要信息，需要重视对待。在系统中，不可见的数据分为以下几部分。

（1）已被删除的数据

系统中被删除的数据是可以用十六进制编辑器手动恢复的。一个基于 Windows 平台的文件被删除后，其实只是将目录项的第一个字母改为一个特殊字符，然后将文件占用的簇标记为空闲状态，而事实上文件中的数据依旧存储在磁盘上。同样，MS-DOS 删除文件的动作也没有真正将文件删除，只是标记这些空间可供重新编制，因此给数据恢复提供了机会。

（2）隐藏的文件

数据隐藏是取证分析中需要面对的一个重大问题。通常有两种隐藏的情况。一种情况是通过某些软件，可以将文件设定为隐藏状态。另一种情况是操作系统会对用户隐藏某些文件和文件名，尤其是系统文件，因为对系统文件的误操作可能导致系统不能正常运行，事实上用户不需要知道这些系统文件的具体作用就能进行系统操作。

基于以上原因，侦查员在侦查时应谨慎对待系统内的隐藏程序，隐藏的数据可以帮助侦查员挖掘更深层次的线索。

（3）坏块

所谓坏块就是硬盘中不可靠的存储区域，包含大量不良磁道，这些磁道将被列举在不良磁道列表中，任何区域的硬盘都无法使用这些磁道。当然这些“不良磁道”也有可能是好的，不过操作系统不会在这些磁道上面进行读或写的操作，所以犯罪分子就有可能将一些好的磁道标记成“坏”的，从而存储信息并达到隐藏的目的。因此侦查员对所有的“不良磁道”进行检查之前，不要格式化磁盘，因为这样有可能会使“不良磁道”的隐藏信息丢失。

（4）隐写术

隐写术是一种隐藏信息方式，用于防止信息被检测的技术。隐写是一种古老的工艺，用到计算机技术上，即将要保护的信息内嵌至文本、图像或视频等具有大信息量的文件中，使其他人不知道该信息的存在，主要目的就在于分散其他人对隐藏信息的注意力。因此，为了应对这种情况，侦查员在取证调查时就应该将搜查的范围扩大。

2. 操作系统的证据分析

很多取证工具都是针对特定平台的，事实上侦查员也更喜欢在特定的平台上工作。下面介绍针对不同操作系统的取证分析过程。

（1）Microsoft 文件系统

大多数计算机取证工具都运用在 Microsoft 文件系统，在该文件系统下的侦查分析需

要做到以下几点。

- 在对硬盘信息进行映像之前，要对分析平台的所有文件进行病毒扫描。
- 在建立硬盘映像之后，继续运行病毒扫描，包括硬盘驱动器的复本。
- 恢复所有删除的文件，将其保管到一个安全的位置。
- 对所有恢复的证据进行分析和处理。

（2）UNIX 和 Linux 文件系统

尽管用于 Linux 文件系统的取证工具还很少，但目前还是出现了一些优秀的 Linux 文件系统取证工具，如 TCT、CTCUTILs 和 TASK。

值得注意的是，由于 Linux 和 UNIX 系统一般用于服务器，因此很多时候侦查员必须处理实时系统。当处理此类系统时，侦查员的首要任务是维护系统中正在运行的所有数据，保护系统中运行程序的状态。具体的运行数据包括控制信息、运行的程序、网络连接信息、系统内存数据等。

13.3 网络取证

对于网络取证来说，已经有一套既定的程序来处理入侵事件。

入侵分析

入侵分析就是对端口扫描以及后门、间谍软件或木马等事件进行处理，及时发现破坏系统安全的行为。

网络安全的最大危险就是忽视系统所面临的威胁。黑客总是在网络攻防中占据主动地位，会在攻击后故意隐藏作案工具。如果不进行入侵分析的话，就不会被检测到这些入侵工具，而入侵分析的目的就是回答以下问题：谁进入了系统，采取何种方式进入系统，发生了什么事件，该事件中取得了哪些教训，能否避免同种事件再次发生。

完整的入侵分析需要一个完备知识储备小组全面分析所有的网络信息来确定证据数据的位置。证据可能存在于网络中的任意位置，包括路由器、防火墙、FTP 与 DNS 服务器文件、入侵检测系统的日志文件、系统日志文件和服务器的硬盘驱动器等。

入侵分析的主要功能是收集数据与分析数据，一般提供 4 种服务：事故应急响应预案、应急响应、入侵数据的技术性分析、攻击工具的逆向追踪。最后分析得到的数据都应存放于安全的存储空间内。

1．应急响应预案

应急响应预案应该包括 3 部分：监视与警报、修复与报告、追捕与检举。在监视与警报环节中，当有安全事件发生时，系统会向负责方进行报警，很多系统都已经达到实时监控与报告的能力；修复与报告的目的就是尽快将受损的系统恢复到受损状态之前，这需要快速识别入侵并修复所有已查明的弱点或及时阻止攻击并将该事件上报给责任主体；最后一个环节是追捕与检举，目的在于对事件进行监控，当入侵发生时及时搜集证据，并将证据直接上报给执法部门。

响应预案应列举出需要采用的程序并为组织成员提供必要的训练，使每个员工都明确自己要做什么。同时还应说明安全事件的优先级及需要的关注程度。响应预案是很重要的，响应预案设计得合理，可以清楚地说明哪些系统环境有可能引起安全事件，事件发生应该采取哪些措施。

应急响应预案最终应包括一系列的文档，以记录系统的行为活动，事发前系统的配置信息，以及其他一些相关信息等，如接触系统的人员名单及人员行为、工具的使用及工具使用者。

2. 应急响应

事件应急响应是安全事件发生后系统必须执行的安全行为的一部分。在应急响应中，有两个部分是最重要的——事件报告与事件控制。在事件报告中，侦查员需要了解以下几点：最先发现事件的人是谁，首先采取了哪些响应措施。一般来说首先采取响应措施的一定是第一个发现安全事件的人。事件的通知程序需要被纳入应急响应的预案中。应急响应小组可以获得准确信息，而且小组内的成员都具备处理安全事件的知识与技能，这些能够有效帮助侦查员进行工作。

事件控制就是要尽可能地阻止事件继续进行，减小事件带来的影响。事件控制对侦查员也很重要，因为其可以有效地控制系统的受损程度和受影响的系统数量。事件控制机制分为以下几个步骤：确定受影响的系统，拒绝攻击者访问，移除流氓进程，重新获取控制。侦查员应格外注意“重新获取控制”这一步，因为重新获得控制后系统就会恢复到原有的状态，造成线索的丢失，所以在获取控制前应首先锁定攻击者。

侦查员收集完证据后，要开始对系统进行重建，具体措施包括备份、安全补丁和程序重装。由于攻击有可能来源于外部也有可能来源于内部，因此事件控制过程一定要谨慎进行，防止罪犯处于组织内部中。

3. 入侵技术分析

网络侦查中最困难最耗时的环节就是对入侵行为和入侵数据进行技术分析。不同于计算机侦查取证，网络取证的大部分证据都不在一个主机或一个存储设备中，需要搜索大量的硬盘驱动器和大量的计算机。

网络取证中必须分析网络信息才能确认线索信息所在的位置。

网络中最为重要的信息来源是网络服务提供商（ISP），因为 ISP 记录着关于网络连接的大量信息。进行网络连接时，首先要经过认证，然后通过 DHCP 服务器动态分配 IP 地址后才能进行。其中认证是由 RADIUS 进行的，每认证一个连接后，RADIUS 都会将其记录下来，以便日后追查线索。RADIUS 的记录有连接分配的 IP 地址、连接的时间、连接者的号码、登录名等。ISP 将这些信息存储起来，存储时间一般为一年。

另外一个重要的信息就是电子邮件，因为邮件上注明了邮件的发信人地址和收信人地址，可以提供很多线索。另外，为了提高电子邮件的可行性，PGP 等技术得到了广泛应用，在邮件服务器中会保存具体的信息日志，这些也可以给调查员在侦查取证时提供很多帮助。

4. 逆向追踪

通常防范黑客的技术就是抓取一个有问题的数据包，然后对其进行分析，从而了解数据包的工作方式与原理，最终达到防御的目的。这也常用于反病毒技术中，通过抓取病毒特征签名学习病毒的工作方式，最终推出具体的反病毒方案。

13.4 取证工具

本节将介绍一些传统的侦查取证工具。侦查员不仅要选择可信的工具，还必须在进行工作前就对这些工具有充分的熟悉，确保能够在侦查过程中熟练使用工具。

事实上，网络取证工具与计算机取证工具是有所不同的，网络取证工具可能同时被侦查员和黑客使用，而计算机取证工具基本只用于计算机取证。

13.4.1 计算机取证工具

目前，计算机取证工具分为两类：基于软件的取证工具和基于硬件的取证工具。

1. 基于软件的取证工具

大多数取证工具主要用于证据恢复和镜像，分类如下。

- **查看程序** 报告系统盘上的系统文件和文件类型。
- **驱动器镜像** 普通的文件复制工具容易错过隐藏数据，而取证软件可以捕获所有闲置的空间，未分配领域等，从而避免漏掉隐藏数据。
- **磁盘擦** 用于强力清除磁盘中的所有内容。
- **信息检索** 通过键入关键字对大量数据快速遍历以寻找线索。

2. 基于硬件的取证工具

目前大部分取证工具是基于软件的，但同时有一些取证工具是基于硬件的。这些工具可能是固定的，也可能是便携或轻量级的。轻量级的工作站主要是基于笔记本电脑的。具体使用哪种工具要根据作案现场的环境和取证的要求。基于硬件的工具还包括写阻断器，该工具可以使侦查员在不关闭系统的情况下对硬件驱动器进行移除和重连接操作。

13.4.2 网络取证工具

常见的网络取证工具有 tcpdump 或 strings 命令。tcpdump 可以在大量信息中过滤个别符合条件的数据包，strings 命令可以根据网络数据传递相应的信息，例如 Snort 就可以根据特定的网络条件来生成警报或其他操作。

然而，如果调查人员对要调查的系统不甚了解的话，那么调查工作将变得很困难。在这种情况下，需要借助一些通用工具。侦查员分析证据的能力会被系统的权限所限制。

大部分商用的取证工具在网络中通过监控网络中每个端口的流量来监控内部、外部的网络数据，通过这些数据就可以知道网络上的用户行为与行为对象。

监控行为中的预警情报收集技术称为“侦查探针”，现在很多标准的取证工具如 tcpdump 都提供这些探针，当然网络中的探针也有可能来自其他的网络监控设备，如防火墙，入侵检测系统。

习　　题

一、选择题

1. 犯罪侦查 3 个核心元素中不包括下列哪一项？（　　）
   A. 与案件有关的材料
   B. 案件材料的合法性
   C. 案件材料的逻辑性
   D. 线索材料

2. 通过对校验和进行加密来判断数据是否有更改的检验方法叫做什么？（　　）
   A. AHSH 算法
   B. SHAH 算法
   C. SHHA 算法
   D. HASH 算法

二、问答题

1. 简述计算机取证的含义。
2. 简述计算机取证的技术及其过程。
3. 思考如何使用取证工具进行网络取证。

课后实践与思考

计算机取证工具使用方法介绍

一、评价使用计算机取证工具的需求

利用万能的、灵活的、精力充沛的操作系统、文件系统、版本容量、自动化的功能。

二、掌握好所要分析的应用文件的种类

计算机取证工具的种类如下。

- **硬件取证工具**　从单一功能的成分到复杂的计算机系统和服务。
- **软件取证工具**　类型、命令行。
- **图形用户界面**　经常用于将数据从嫌疑人的光驱上变成图像文件。

专用的（SafeBack－Disk acquisition only），普遍的（Encase，FTK）

Digital Intelligence UltraKit

Digital Intelligence F.R.E.D.（Forensic Recovery of Evidence Device）

Digital Intelligence F.R.E.D.D.I.E　Forensic Recovery of Evidence Device（Diminutive Interrogation Equipment）

Digital Intelligence FRED L

Digital Intelligence FRED Sr

Digital Intelligence FRED M

DIBS USA

三、计算机取证软件的工作

为了得到罪犯不法记录的证据，计算机取证要求得到的可能是数据的逻辑或物理版本格式，或者是用户图形界面，或者是命令行的获取，以及远距离的信息获取。其中物理数据要求得到的是整个驱动装置的信息，逻辑数据是磁盘的部分信息。

计算机取证工具的用途：获取、验证和描述、抽取、重建、报告。

1．获取

（1）逻辑数据版本（copy）。

- ❑ 数据获取格式
- ❑ 命令行获取
- ❑ 图形用户界面获取
- ❑ 远距离的获取

（2）校验。

（3）两种数据复制方法在软件取证中的应用。

- ❑ 整个磁盘的物理复制
- ❑ 部分磁盘的逻辑复制

（4）千变万化的磁盘取证形式。

从原始数据到卖主专用的私有压缩数据。

（5）使用任何十六进制的编辑器都可以浏览到未经修改的文件夹的内容。

（6）现在能买到的获取工具都是具有将一个文件分割到好几个小部分的特征。

（7）每一种计算机取证工具都有一种校验数据复制过程的功能。

2．辨别和描述

（1）验证

保证所复制的数据的完整性。

（2）数据的描述

包括分类和调查全部的调查数据。

（3）验证使所有的描述成为正确的

如果没有调查，那么就不可能说明数据的作用。

（4）其他的一些功能

- ❑ 哈希值，如 CRC-32、MD5、Secure Hash Algorithms。
- ❑ 过滤，即建立在哈希值的基础上的过滤。
- ❑ 分析文件的标题。根据它们的类型对文件进行分类。
- ❑ 全国软件参考图书馆（NSRL）编写了已知的文件名单，为各种各样 OSs、应用和图象。
- ❑ 很多的计算机取证工具项目中包含一些普通的标题评估列表，如这样的文件：可以很清楚一个文件具有这种文件扩展名是否正确。
- ❑ 大多数的取证工具能验证标题的评估过程。

3．抽取、析出

很多时候人们会问为什么要进行数据的抽取，下面是抽取数据的重要性。

（1）在计算机调查中恢复计算机原本的工作内容。

（2）有时候在调查的过程中需要掌握很多的工作内容。

（3）恢复数据往往在调查中是第一步。

（4）其他的一些作用。

❑ **数据浏览**

在进行数据浏览的过程中，应知道：①数据被怎样的浏览时取决于使用的是什么样的工具；②磁盘间谍——逻辑结构；③装入/FTK——多样性浏览器。

❑ **关键字搜查**

在关键字的搜索的过程中，是很容易就可以加快分析或调查的速度的，但是在使用关键字的搜索的过程中，也需要掌握：①保证恢复关键字的准确性；②这个过程可能会非常的耗费时间并且很发杂；③必须明确使用的工具是否能完成直接搜索或调查；④使用索引可以提升搜索的速度（但是这需要更长的分析时间）。

❑ **解压、减压**

这部分工作的内容：①FTK 能解压档案文件和封锁的文件，而装入技术却不行；②装入技术要求创建原本，而解压技术则没有此种规则。

❑ **刻录**

下面是一些刻录的要求和内容以及其重要性：①重建已删除的文件中或其他的一些没有定位空间的图标的信息；②可能需要用到一些文件标题中的一些信息。

❑ **翻译、解密**

下面是对解密技术的一些相关的技术要求：①很有可能在文件上，隔离空间或磁盘上的一些数据等都很重要；②许多密码补救工具有引起密码列出是潜在的一个特点（FTK），引起密码库的被攻击；③如果密码库遭到工具，就可能会遭遇暴力攻击的经历。

❑ **做标签**

在第一次找到证据的时候就做一下标签，以方便下来的引用或报告的工作。

4．重构、恢复机制

（1）重新构建犯罪嫌疑人的驱动等来显示在犯罪或事故的时间段内，嫌疑人在干什么？

（2）其他的一些功能如下。

❑ 磁盘对磁盘的复制

❑ 镜像对磁盘的复制

❑ 部分对部分的复制

❑ 镜像对部分的复制

（3）一些被用作于镜像对磁盘的工具：SafeBack、SnapBack、EnCase、FTK Imager、ProDiscover。

5．报告

（1）为了完成对磁盘取证的分析和测试，需要建立一个报告。

（2）一些其他的作用。

❑ 原报告

❑ 报告大概的事件

（3）这份报告可以作为调查的最终的报告结果。

6．计算机取证工具的一些其他的内容

（1）考虑的内容如下。

- 灵活性
- 可靠性
- 可扩展性
- 在你的工具中表留一个老版本的库

（2）建立一个软件的库，包括老版本的取证工具设施、操作系统和其他的一些项目。

（3）基本的一些策略：命令行，如 DOS、Linux/UNIX 或者图形用户界面。

四、计算机软件取证工具

（1）第一个可以从封装的粗盘里或硬盘中读取并分析数据的工具是用于 IBM 个人电脑的文件系统的 MS-DOS 工具。

（2）诺顿的磁盘编辑器。第一个 MS-DOS 工具用于计算机调查的一种工具。

（3）优点。命令行工具需要很少的文件系统资源，在一种很小的形势下运行。

（4）*NIX 的命令行工具。此种工具收到越来越多的家庭用户的青睐，很多不同版本的操作系统可以使用。

（5）*NIX 取证工具。

- ***NIX 平台**　在很久之前就成为命令行操作系统的基础。
- **SMART**　很多版本的 Linux 可以被安装，Linux 可以分析很多 SMART 的文件系统，很多的插入设施要求敏捷度，SMART 的十六进制浏览器中有一些其他的有用的选择。
- **Helix**　一种最简单开始适配器，你可以在一个活动的 Windows 系统下载它。
- **Autopsy**　是图形用户界面或者是浏览器用作于使用 SleuthKit's 的工具。
- **SleuthKit**　是 Linux 取证工具。
- **Knoopix-STD**　一种安全措施，包括计算机或者网络取证的收集。

（6）其他的图形用户界面取证工具。

- 计算机取证的调查分类。
- 帮助开始的调查。
- 它们大多数的是以一整套的工具出现的。
- 优点：很容易使用，可以多任务处理，没有必要学习旧的操作系统。
- 缺点：过度的需要资源，产生必然的一些问题，产生工具的依赖性。

五、计算机硬件取证工具

为什么会产生计算机的硬件取证工具，相信很多的计算机取证人员都是相当的清楚的：随着技术的变化的越来越快，硬件最终还是出现了问题，如日程安排上的设备的替代，当计划预算时就要考虑如果硬件不再可以用、咨询和维护的费用、设备的更新的费用，这些都在一步步地将计算机硬件取证工具牵扯上计算机的取证的舞台。

六、取证的工作区或其环境

在安全维护人员熟悉了解计算机取证的不同的类型之后，还需要很好地掌握取证的工具，以便在不同的环境中选择最好最实用的取证设备，只有这样才能在损失或花费最小的情况下保证取得证据是准确的、完整的。

（1）在考虑计算机取证前，在考虑取证的环境中需要做到以下的几点要求。

- 认真地想清楚到底需要的是什么？
- 得到的证据的形态：静态的；动态的，轻便的。
- 衡量一下所需要的和计算机系统可以处理的东西是否适应。

（2）具体的集中取证的环境。

- 警务处的实验室：需要非常多的选择，用几台个人的计算机的去构造。
- 4人合作的实验室：衡量一下唯一的一种在组织中使用的系统的类型。
- 除了一个软件实验室还要保留一个硬件实验室。

（3）分析一下取证环境的程度。

- 它并不是听起来那么具有难度。
- 优点：满足需求的同时做到节省开支。
- 缺点：很难找到问题支持的物件，如果不小心，很有可能会造成很大的浪费。
- 此外还必须认证到底想要去分析的是什么，然后可根据需求找到卖主去购买，当工具出现问题时卖主很可能解决燃眉之急。
- 运用一个写阻止的工具：可以很容易地阻止使用者使用任何的写工具。

（4）适用于取证工作区的一些推荐的方法

- 要知道数据获取要在什么地方进行。
- 知道数据获取的技术：USB 2.0，firewire 3。
- 扩展设备需求，其中还必须使用电池来提供能量。
- 如果有受限制的预算，推荐使用PCs等一些其他的方法。

七、取证的一些常见的工具

就目前来看，在遭受攻击的单位中，有很多人员还不知道自己遭受了攻击。许多人相信，主要的攻击来自于公司外部。其实，很多重大的损害来自于内部。

那么，安全人员面临的挑战就是如何找到这些攻击，并判断其进入系统的方法和途径。因为桌面用户用得最多的是Windows系统，所以要看几个可以针对这种系统进行取证的简单工具。

下面列举了国外5款著名免费计算机取证工具。

1．Live View

使用此软件首要的一点是为用户的现有系统创建一个虚拟机，还要结合使用开源的Live View软件。此软件会检测用户的系统，如果没有检测到安装有Vmware Server 1.x或工作站版本的虚拟软件，它会为用户下载一个。

Live View是一个基于Java的图形化的取证工具，它可以创建原始磁盘映像或物理磁盘的一个VMware虚拟机。它准许取证人员可以启动这个镜像或磁盘，并获得一个交

互性的、用户级的环境视图。因为对磁盘的所有更改都被写入一个独立的文件，检查人员可以很快地恢复到磁盘的原始状态。其最终的结果是用户不需要创建额外的磁盘映象来构建虚拟机。

不过，目前此软件仅支持 Windows 2003、XP、2000 等系统，对 Linux 也仅是有限支持。

2．Opened FilesView

这是一款可以列示系统上所有基于本地或网络的文件。此软件只有 82.88KB，其安装后的界面如图 13-1 所示。

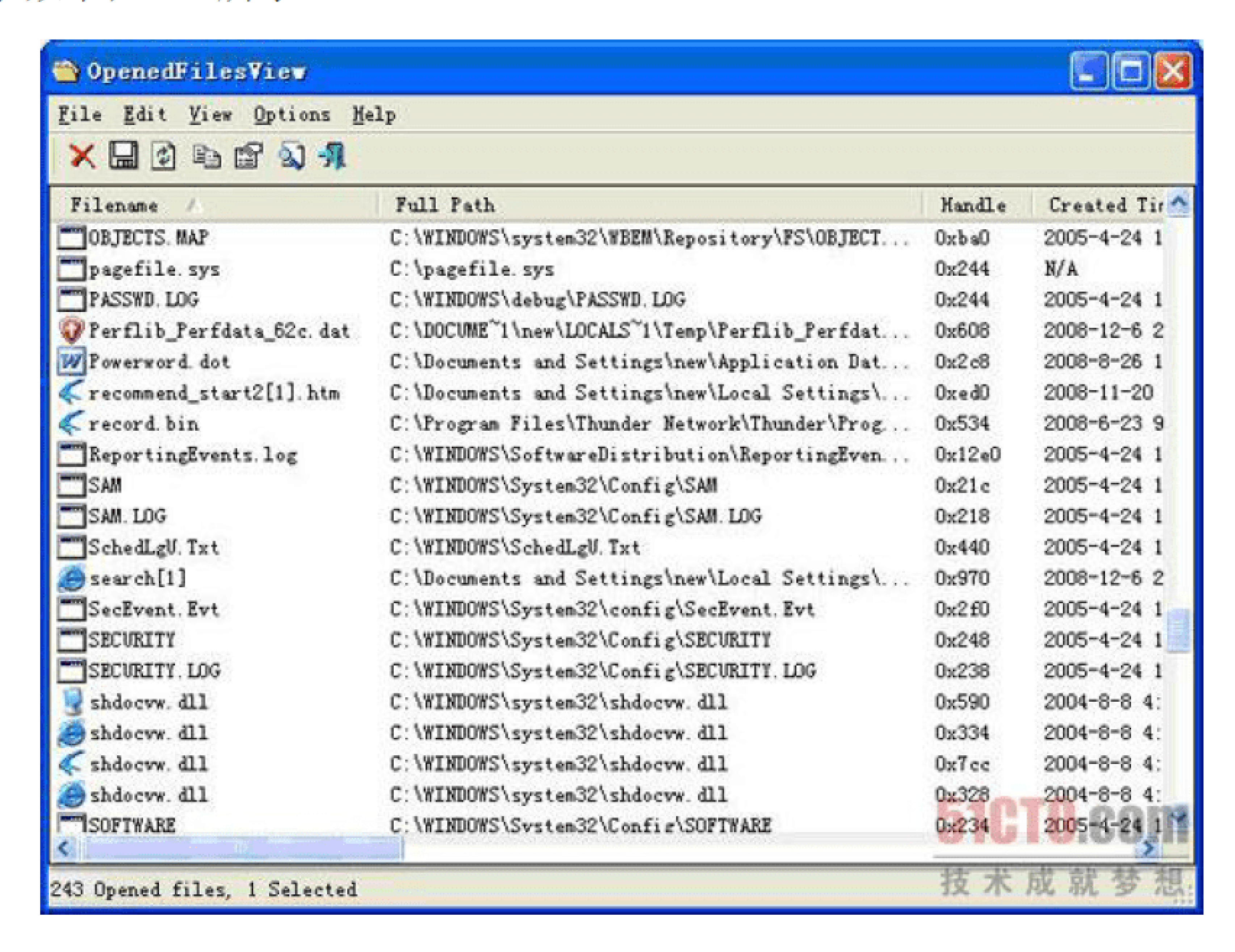


图 13-1 Opened Files View 的主界面

此软件可穷举系统中的所有句柄。在过滤了非句柄之后，它使用临时设备驱动程序来从内核存储区读取每一个句柄。在用户从该软件退出之后，这个设备驱动程序又可以自动地将其从系统中释放。显然，在这一点上，这是其他的任务管理程序所不能及的。

如果用户试图删除或移动或打开一个文件时，收到了类似于下面的错误消息，那么此软件就极为有用："无法删除*共享文件，源文件或目标文件正在使用"。

此外，如果与网络连接的过程中，打开此软件可以监视网络进程，如果用户怀疑某进程有问题，可以在其上单击，如图 13-2 所示。

软件对文件的多种属性进行了描述，如句柄、进程 ID、删除共享等。在确信了某句柄是可疑句柄之后，可以单击 OK 按钮。再次在此文件上右击，选择 Kill Processes Of Selected Files 命令。

3．HELIX

此工具就是大名鼎鼎的 Ubuntu Linux 的定制版本。它不仅是一个可启动的 CD 工具，还可以通过它启动进入一个包含内核、优秀的硬件检测程序以及一些专用的事件响应和取证方面的应用程序。

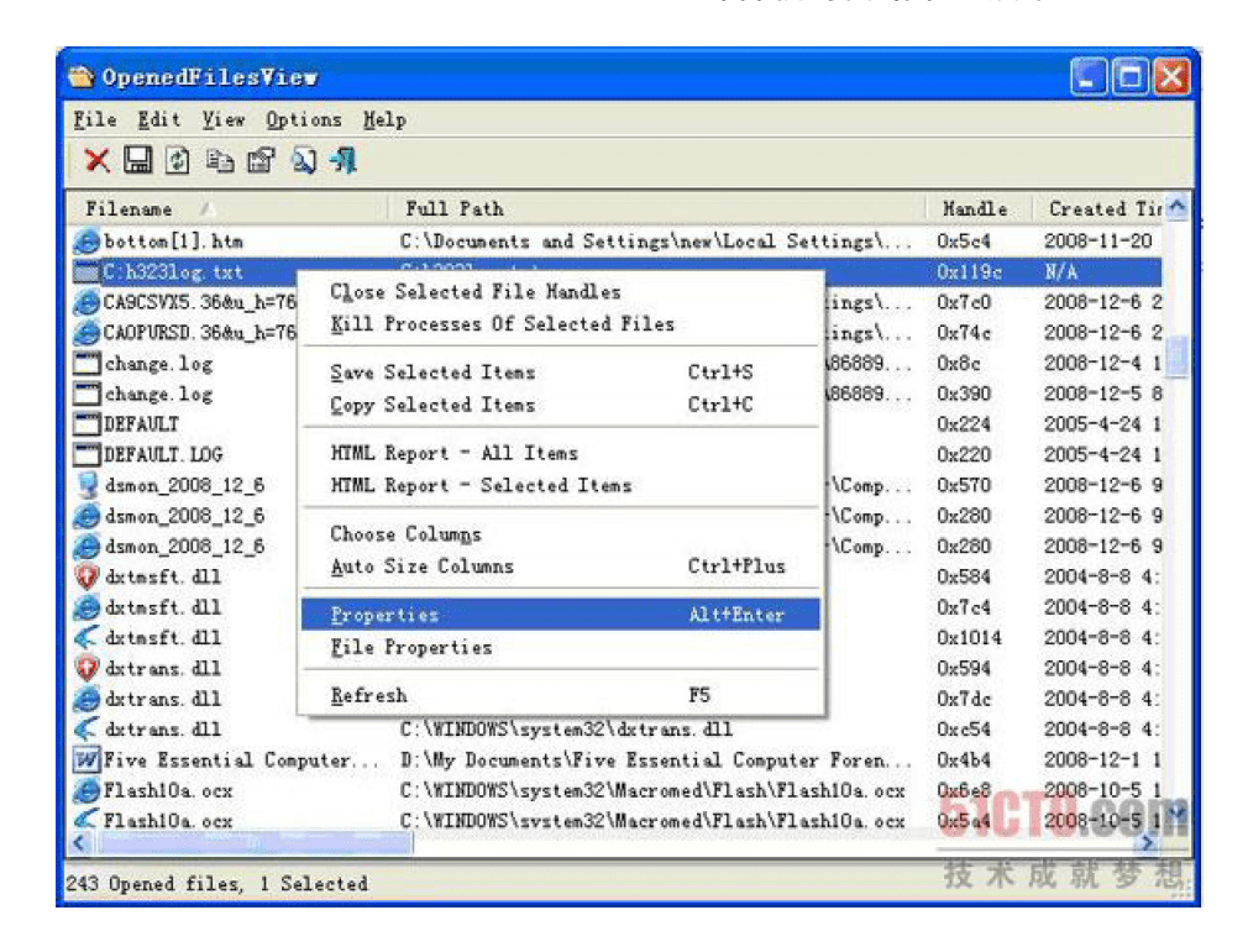


图 13-2　网络进程监视

它可被用于检查磁盘，看有什么发生了变化。系统的取证关键是找到什么方面受到了损害。知道受到了攻击是一个方面，而找出这些攻击者对系统做了哪些手脚是至关重要的。这正是此工具的长处所在。其工作界面如图 13-3 和图 13-4 所示。



图 13-3　HELIX 工作界面 1

图 13-4　HELIX 工作界面 2

第 14 章　操作系统安全

本章学习重点：

- 理解操作系统安全的特点和好处
- 理解 Windows 和 UNIX 的基本安全设计
- 认识和处理常见的安全风险
- 理解系统备份的重要性和危险
- 识别数据风险，分析控制每一种风险的代价
- 根据对系统的作用大小对系统安全风险进行排序

操作系统是位于底层硬件与应用程序之间的一层软件，是用户与硬件设备沟通的桥梁，支持用户的各种操作。操作系统是访问计算机资源时用户和应用程序相遇的中间实体，为用户提供了访问数据和其他资源的服务以及路径。如果操作系统是不安全的，其所处理的任何资源的安全就得不到保证。

无论实施怎样的安全控制，用户首先需要理解操作系统是如何保证资源安全的。然后，以此为基础构建更加安全的平台。如果对操作系统如何解决安全问题一无所知，就很难实施安全的控制。本章主要介绍基本的操作系统安全并且讨论如何识别常见的系统漏洞。

14.1　操作系统安全基础

14.1.1　操作系统安全术语和概念

操作系统最基本的作用就是使用户程序受控地访问计算机硬件组件。这些组件包括主存储器、二级存储器，处理器、输入/输出设备以及网络组件。表 14-1 给出了一个操作系统管理的主要系统资源。

表 14-1　操作系统管理的主要系统资源

系统资源	实例	描述
主存储器	随机存取存储器（RAM）	计算机内的物理存储器，易被处理器单元访问。具有易失性，断电之后，存储器内的内容就会丢失
二级存储器	磁盘、软盘、CD-ROM、磁带	数据的非易失存储器。包括固定和移动的，随机访问的和顺序的
处理器	中央处理器（CPU）	命令执行地点。一台计算机可以有几个 CPU 和另外几个特殊功能的处理器
输入/输出设备	键盘、显示器、打印机、鼠标、扫描仪	从计算机外部收集数据或将数据输出到计算机外部的所有设备
网络组件	网络接口卡（NIC）	连接计算机总线和外部网络的硬件设备，可以是电缆连接或无线连接

操作系统的另一个重要功能是保障内部的资源和数据的安全性。旧版操作系统更关注于数据的保密性，确保只有授权的用户可以看到敏感数据。随着操作系统和网络的发展，有更多的安全事件需要关心。现在的操作系统不只能实施严格的访问控制，除了保密性，还要确保数据的完整性和可用性。数据完整性保证受保护的数据不被非授权的更改。数据可用性保证所有的机制适宜地工作，使得用户在任何时候都能访问到所需资源。

操作系统必须执行 4 种基本的安全功能来支持保密性、完整性以及数据的可用性：识别用户，限制对授权资源的访问，记录用户活动，保证和其他计算机以及设备的连接。其中，最后一个功能被极大简化了。操作系统不仅要保证存储数据的安全，还必须能提供一种方式使得数据能够安全地发送到另外一个系统。这 4 种功能组成了操作系统职责的核心，至少是和安全相关职责的核心。在以下的部分，将会讨论这些功能是如何应用的。

14.1.2　系统安全规划

系统安全规划着眼于 4 种基本安全功能。①系统识别用户。这可以通过很多种方式实现，已经在前面讨论过了。不管系统使用什么样的识别方法，能够确保访问控制正确地识别用户。②认证用户。认证通常要求用户提供其他一些信息来证明他们就是所声称的那些人。③在识别和认证一个用户之后，就是为用户授权一些特定的访问权限。这种授权是基于规则的，可以根据用户的身份，角色，或者其他一些和客体安全标签相关的准则来授予。操作系统的责任不仅是限制授权主体对客体的访问，还要记录访问过程，以便于之后的审计。同时，还必须丢弃不合法的请求使得合法的请求能够被及时处理。

通常情况下，操作系统的安全功能是分层的。控制安全的软件位于用户请求和访问资源的驱动程序之间。拦截所有用户请求的层次叫做访问监控器，执行每一个客体请求的授权工作，由一系列方法和函数构成。访问监控器是安全内核的一部分，安全内核是操作系统中处理所有安全事件的部分。安全内核处理授权，以及审计问题。尽管安全内核是核心操作系统的一部分，还是能够通过与外部组件结合扩展自己的功能。

安全内核授权了一个资源请求之后，这个请求就被传递给目标操作系统层。目前的操作系统至少有两个不同的层次——内核层和用户层。应用程序运行在操作系统的用户层上面。用户层执行的指令运行在受限的 CPU 水平上。通常，用户层程序不会执行一些潜在的危险指令。通常，内核级程序是那些可以执行更高权限 CPU 指令的程序。执行内核级程序需要一个更高的权限，因为其结果往往直接影响硬件驱动和内存。由于以内核模式运行程序的潜在的危险性，所以通常只有关键的操作系统功能才使用这种程序。

14.1.3　内置安全子系统和机制

每一种现代的操作系统都拥有最基本的安全机制。事实上，当代操作系统具有非常复杂的安全功能。为了便于安装、易于用户使用，大多数的操作系统默认的安全等级都比较低。因此，对于一个新的操作系统就需要一定的工作来对安全水平进行升级。这个增加安全等级的过程通常叫做加固。加固的过程就是找出操作系统中已知的漏洞，并试

图消灭或减缓这些漏洞。

最常见的操作系统安全子系统是身份识别系统和认证系统。除了极少数的例外，用户和信息系统的第一个交互就是登录系统。尽管工作站可能不需要登录，但是联网计算机和服务器请求用户提供用户名还是很常见的。用户提供了用户名之后，操作系统往往会提示用户出示一个口令。在系统内部存储的用户数据库中，用户名和口令被核实，然后决定接受或拒绝这个用户。在大多数现代操作系统中，这个简单的过程是最常见的。

另外一种方法就要复杂得多。用户需要使用一张智能卡或生物设备来向操作系统提供认证信息。两种方法的思想是一致的，即用户向操作系统出示证书，操作系统对这些证书进行核实。核实之后，操作系统决定用户可以进行哪些操作。大多数情况下，操作系统或是以一个事先规定好的认证等级认证用户，或是拒绝用户的访问请求。在某些情况下（比如用户重复访问失败），操作系统就可能锁定有问题的用户账户，要求其他管理机构来解决这个问题。随着操作系统的成熟，越来越多的高端功能被加载进来。除了基本的用户名和口令功能，许多新型的操作系统都具有单点登录和远程认证解决方案。例如，Kerberos 就是一个适用于大多数 UNIX 变体的网络认证协议，现在也被许多微软产品所使用。

每一个操作系统都有独特的内置安全子系统，但在所有当代操作系统中一般的身份识别以及认证协议是很常见的。对用户进行了认证控制之后，各个操作系统的差异就变得明显了。用户开始加固系统之前，要确保系统提供的服务已经很满意了。适当的操作系统安全应用可能会更加的安全更加的高效。

14.2 操作系统安全原则与实践

一个安全的操作系统是一系列可靠计划的结果。安全计划是以了解自己系统的安全风险开始的。风险评估就是对用户数据的风险进行识别以及划分等级。用户需要对每一个风险进行评估和分析，并找到一种或多种技术来解决这个风险。

用户在找到所有的系统风险以及相应的处理方法之后，就可以开始应用风险控制技术。应用控制技术的过程增加了系统总的安全性，使得系统更不容易被渗透。这个过程应该在用户仔细研究自己组织的风险之后再实施。不要盲从“10 个步骤轻松加固你的电脑”这样的清单（尽管这样比什么都不做要好）。这样的清单中所包含的步骤可能涵盖了大多数系统漏洞，但是在实施控制技术之前，用户需要了解自己的系统到底有哪些特别的漏洞。

用户在对操作系统加固之后，就需要检测加固的结果。要记住附加的控制限制了对客体的访问，因此，这就可能在一定程度上影响系统的运行。在应用或更改了安全控制之后，要对所有的系统访问操作进行全面的检查。下一步的工作是安全培训和通用操作系统操作。对系统的任何更改都要提供培训。

这些原则对于所有的操作系统都是通用的。识别风险，然后选择最合适的控制技术来处理每一个风险。在完成控制技术的应用步骤之后，对每个控制手段进行评估以确保不会影响系统其他部分的性能。

14.3 Windows 系统安全设计

Windows 安全模式在多种 Windows 产品中是不一样的，差别最大的就是工作站和服务器。这主要是因为各种不同的计算机有着不同的目的。工作站计算机经常作为访问的主体，而服务器计算机是客体。因为人们更关注存储在服务器上的数据，所以本节重点在于 Windows 服务器的安全设计。

Windows 服务器安全是建立在活动目录概念基础上的。Windows 目录服务是使用网络对客体进行寻址和访问的结构。活动目录不是唯一的域服务。其他的服务商，例如 Netscape iPlanet 和 Novell NDS 的产品同样有类似目录服务的功能。域是由管理员创建的网络资源的逻辑组，这些域构成了目录服务构架中的基本组别。网络资源可以是计算机、打印机、用户，甚至是其他的目录对象。域可以分组形成树和森林，形成系统的等级族群。目录服务同样允许域之间构成直接的信任关心，不管它们在森林中的位置。

对系统进行逻辑上的分组使得管理员可以通过组特性对几个客体进行管理，减轻了管理负担。每一个文件，文件夹和打印机都是一个目录服务客体。每一个客体具有相应的任意访问控制列表（DACL），明确了哪个主体可以访问该客体。访问主体可以是用户、用户组或计算机。DACL 限制对客体的访问可以在客体类别、客体或客体属性水平上。因为主体和客体都具有多个层次（例如用户、用户组、计算机），访问控制就会非常灵活，当然也很可能会存在相互矛盾冲突的规则。如果张三被授予修改 Readme.doc 的权限，但是程序员组却没有被授予这样的权限，而张三是程序员组的成员，结果会怎么样呢？因为域控制器使用继承来建立访问控制规则，所以在应用时更明确的规则会起作用。在这个例子中，张三会保留写的权限，因为用户比起组要更明确。然而，如果程序员组已经被明确拒绝访问 Readme.doc，这个结果就会有一些变化。尽管大多数的规则是分层建立的，但是否认规则（Deny rule）是优先执行的。如果程序员组被明确拒绝访问 Readme.doc 文件，只要张三是这个组的一个成员，他就不能访问这个文件了。

继承特性允许规则在域的层次上被确定，运行的时候并不需要太多的管理员维护。管理员应该维护的是和通用访问权限不同的特殊情况。在最初的访问被允许之后，每一个客体能够明确对于主体的权利。目录服务提供了一种构架，能够在网络环境中明确存储、寻址以及请求客体访问信息。实际的客体信息是存储在一个分布式的数据库中的，所以对于认证信息的访问不会造成系统功能瓶颈和单点失败。

对于本地安全或者是域安全，管理员通过微软管理控制台（MMC）来维护个体安全客体的属性。MMC 是定义和维护组策略客体的初级接口，定义了用户组对于特定系统事件的安全设置。图 14-1 给出了对于关闭系统的本地安全策略。

当进行资源请求认证的时候，Windows 通过认证当前的登录用户以及用户的组成员关系来决定是否允许此次请求。在互联网环境中，这些设置可以从域中的客体设置中继承。通过域控制器计算机上的 MMC 以相似的方式来维护更高等级的安全水平。

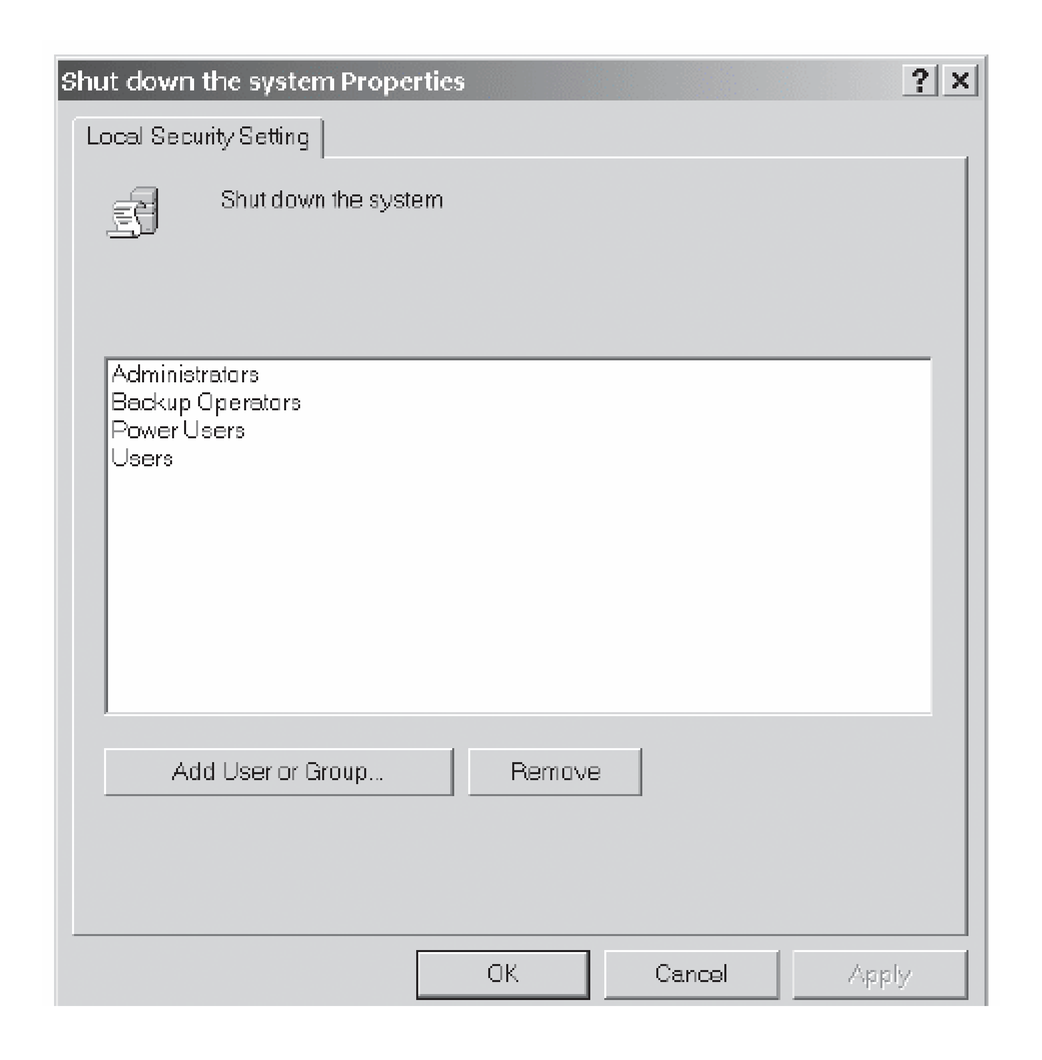


图 14-1　Windows 系统本地安全策略示例

14.4　UNIX 和 Linux 安全设计

Windows 系统把安全和事件及组关联在一起，而 UNIX 和 Linux 系统则是围绕着文件构建基本安全。事实上，在一个 UNIX 系统中，所有的东西都是一个文件（为了简单起见，这里把 UNIX 和 Linux 的变体都称为 UNIX）。在 UNIX 中，文件是文件，设备是文件，目录是文件，甚至运行的程序也是文件。这样就简化了 UNIX 中的许多管理，同样也使得文件权限的管理成为系统管理的关键。UNIX 管理中的主要困难就是和文件权限相关的。因此，先来了解一下 UNIX 的文件系统及文件权限。

在 UNIX 文件系统中，每一个文件都有一个权限，或与之相对应的模式域。这个模式域由 10 个字符组成，明确了这个文件的安全访问特征和其他一些特征。图 14-2 给出了每一种模式域的含义。在这个例子中，客体是一个文件（在第一个域中，没有“d”）。这个文件的权限允许文件所有者读、写、执行这个文件，允许属于这个文件组的用户读、执行这个文件，而其他的用户只能读这个文件。

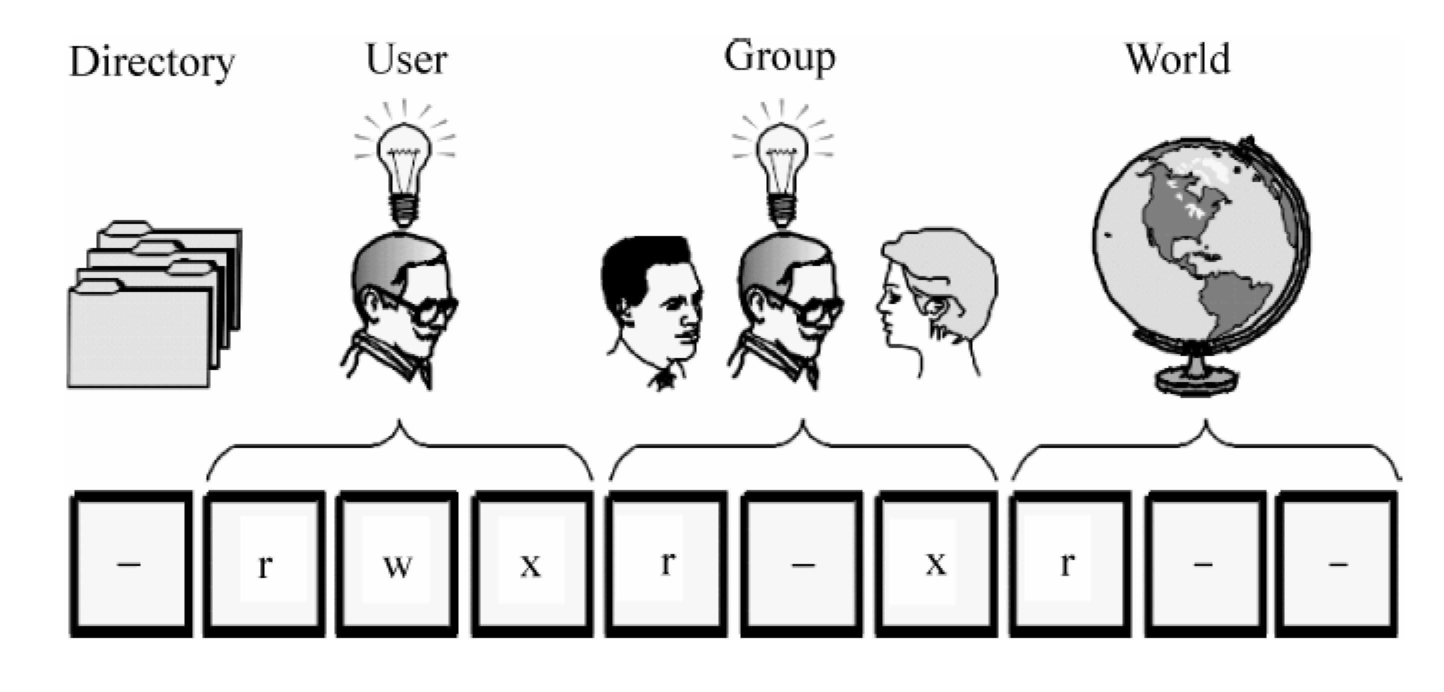


图 14-2　UNIX 系统模式域示例

用户可以利用一系列的命令看到文件的模式域。图 14-3 给出了文件模式域的一个典型列表。

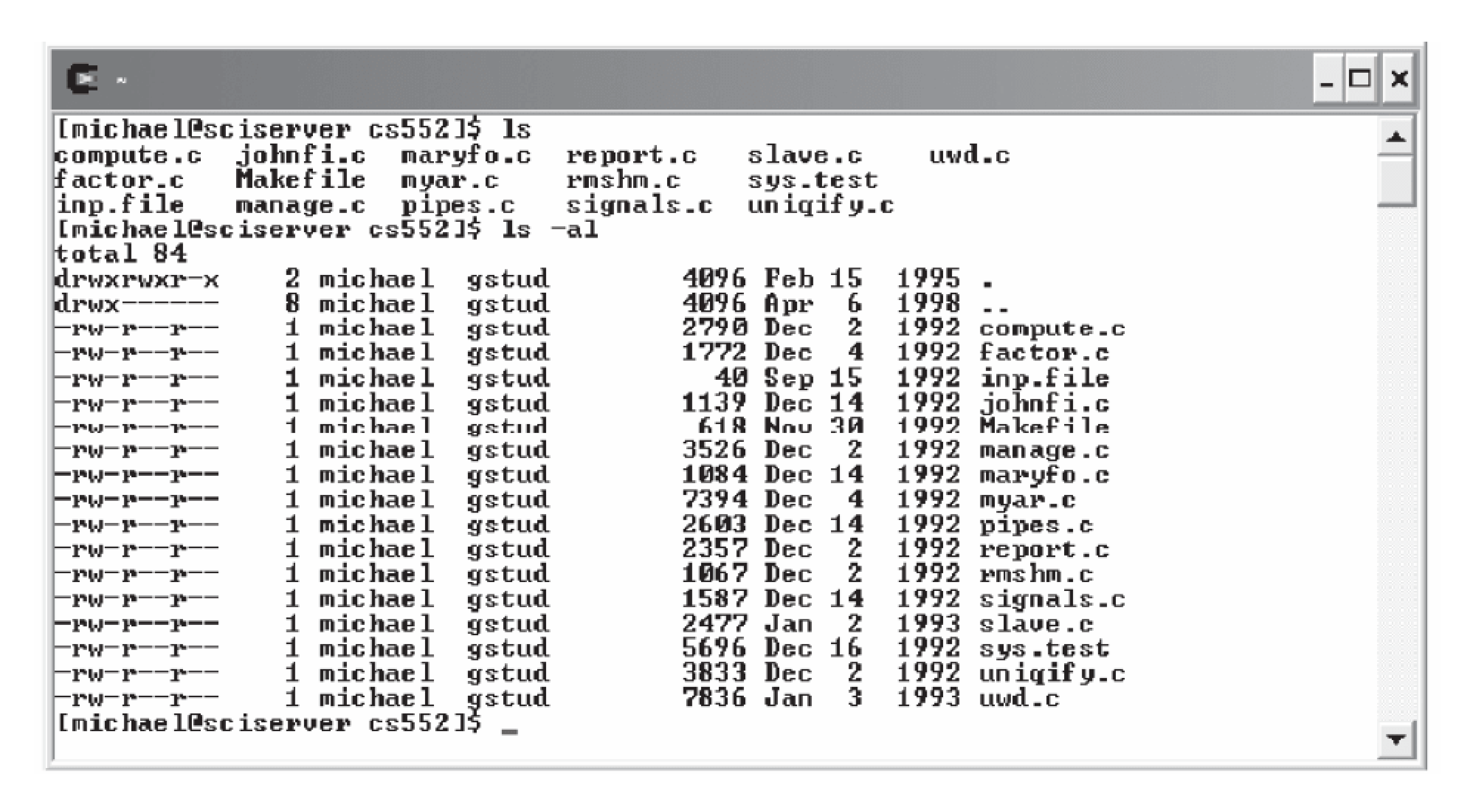


图 14-3 UNIX 系统文件模式域示例

模式域由 4 个部分组成，指出了文件的种类以及文件所有者，文件组以及其他人对文件的访问许可。表 14-2 对模式域的每一个部分进行了描述。

表 14-2 模式域各部分具体描述

在模式域中的位置	可能的取值	描述
第 1 位	-——常规文件 d——目录（directory） l——符号链接（symbolic link） b——块特殊文件（block special file） c——字符特殊文件（character special file）	文件模式域的第一个字符指出了文件类型。这些只是文件类型其中的一部分，文件类型能够影响文件权限如何被应用
2 到 4 位	r——读权限 w——写权限 x——执行权限 -——无权限	文件所有者的访问权限。权限可以组合，例如，rwx 说明文件所有者能够读、写、执行这个文件；而 r--说明用户只能够读这个文件
5 到 7 位	r——读权限 w——写权限 x——执行权限 -——无权限	文件组用户成员的访问权限
8 到 10 位	r——读权限 w——写权限 x——执行权限 -——无权限	一般用户的访问权限

UNIX 把所有这些特征放在一起来构成文件的模式域。例如，考虑下面这个命令行：

```
-rwxrw-r- - 2 michael gstud 7394 Sep 15 14.45 signals.sh
```

这个结果给出了关于 signals.sh 文件的信息。这个文件属于用户 michael 和用户组

gstud。文件的大小是 7394 比特，最后一次修改时间是在 9 月 15 日 14:45。模式域“-rwxrw-r-”，说明文件的所有者能够对这个文件进行读、写、执行（rwx），一个可信组的用户成员可以对这个文件进行读、写（rw-），而其他的用户只能读这个文件（r--）。

注意，所有的文件访问都是通过用户身份和组关系来管理的。UNIX 使用基于身份的访问控制用于基本的资源保护。

14.5 系统备份

如果不包含备份功能，任何的操作系统安全都是不完整的。系统备份是系统局部或全部的复制，通常存储在可移动介质上。其目的是为了向用户正在使用的系统提供一个副本，在原版本丢失的情况下可以使用。可能会有很多种原因导致系统原版本的丢失，服务器遭到攻击导致失效，恶意攻击破坏重要数据，或是硬件失灵。在任何一种情况下，都需要依靠系统的备份来恢复系统的运行。

系统备份可以成为用户系统最好的保护，但也可能是最糟糕的漏洞。保护的作用是很容易理解的。当用户丢失了数据的原始版本，第一个转向的地方就是用户的最新备份。当然，还有许多其他的选择。例如，冗余系统可以提供相同的 coverage 作为备份。这样的系统，成本可能会很高，但恢复的时间通常会很短。对于包含冗余成分的系统，可靠的系统备份向系统提供了一个稳定的二级备份。

备份之所以会成为用户系统的漏洞是因为系统备份通常被创建在可移动的介质上。而介质能够被传输到很远的地方。除非对用户备份的传输途径和存储地点进行严格的物理控制，否则这些备份可能会落入恶意第三方手中。相比较而言，在数据中心得到数据肯定比通过数据备份得到数据要更困难。即使保密性并不是用户最初关心的重点，可是一个完整的系统备份通常包含了足够信息用于攻击者向运行中的系统攻击。

用户创建备份的时候，首先需要做的是检查备份创建的介质是否是好的。很多时候，备份被日复一日地创建在坏的介质上面。如果不花费一定的时间来检查介质的好坏，那就相当于没有做备份。当用户需要使用备份的时候，却发现它们是坏的是一件十分糟糕的事情。制订一个备份的计划表，定期使用新的介质，并对这些介质进行标记，然后把备份存储在一个安全的地方。一个好的备份是恢复计划的主要组成部分。要采取一系列的步骤来保证备份是完整性和安全性。

14.6 典型的系统安全威胁

系统安全的总体目标就是要保护数据免受威胁。对于存储在信息系统里的数据，有很多种的威胁。威胁可能是允许主体超过授权权限，执行一些非授权的行为。或者拒绝一个授权主体访问授权的资源。这个部分将介绍 3 种常见的系统安全威胁。

1. 软件漏洞

第一类安全威胁就是软件漏洞。漏洞可能使软件运行产生预料之外的结果，还可能使软件停止工作，甚至导致软件崩溃。软件开发者负责设计代码时要注重程序的健壮性。

一般来说，对于程序十分精通的设计者设计的代码比起那些对程序一知半解的人设计的代码的可靠性要高的多。

漏洞之所以能够形成安全威胁，是因为其向攻击者提供了入侵系统的机会。软件中的漏洞可能使得用户获得比正常情况更高的权限来运行程序。如果在运行高优先权的指令时程序崩溃，漏洞可能使得攻击者绕过所有的访问控制。攻击者可以使用更高的权限截获数据，侵入系统。

处理这些安全威胁的最好方法就是阻止漏洞的产生。可以通过各种方法来严格限制软件中漏洞的数量，包括训练程序员编写可靠的代码，依照正式的软件开发办法，以及在软件发行之前进行完整的测试。

2. 后门

另一种常见的威胁是后门。后门是能够绕过一些或是全部安全控制的软件进入点。许多软件开发者设置后门是为了避免在软件的开发和测试过程中处理大量的安全控制。但后门也有可能是意外地留下来的。在软件安装之后，后门有可能作为一个秘密进入点被留了下来。即使其目的不是恶意的，但后门的存在确实是一个巨大的安全威胁。后门可以被开发者出于一些不道德的原因来利用，也可以被攻击者发现和使用。无论哪一种方式，都会造成安全威胁。常规的测试应该发现主动探测，当发现后门时，应主动消除。

3. 假冒身份

最后一种常见的威胁是假冒或截获用户身份。目前为止，实现这种威胁最简单的方法是攻破某些人的口令。当获得一个人的用户名和口令之后，就可以通过其身份登录系统。截获一个用户的身份可以有很多方法，包括社会工程学或使用各种技术攻破。在下一个部分，将讨论获取口令的一种方法——击键记录。

除了有关身份窃取的问题，还有其他监控和审计用户活动的问题。如果一个攻击者使用了甲的用户名，那么要把甲与攻击者的行为分开是很困难的。因此，用户一定要保护好自己的用户名和口令。要让用户明白口令安全的重要性。处理假冒身份的最好办法就是采取措施来避免任何身份信息的泄露。

14.7 击键记录

正如上一部分所提到的，击键记录是一种窃取用户已经输入的口令的方法。可以在计算机上安装击键记录软件或硬件，来存储用户的所有击键行为。另外，也可以使用录像机对准用户的键盘进行记录。软件击键监视器是一个驱动程序，需要对操作系统的特权访问来进行安装。硬件设备只需要插入计算机键盘接口上。如果拥有对计算机的物理访问权，硬件设备安装起来最简单。不管种类上的区别，这些监控器的目的就是追踪，并且在日志文件中存储每一个击键行为。一个系统使用击键监视器通常有以下 3 种原因。

- **测试和质量保证** 测试软件时，重复执行相同的任务是很必要的。保存用户的终端输入能够使得多次重复的输入更简单、更精确，剔除了人为操作的错误。这种情况下，使用击键监视器是很常见的。

- **证据收集** 当怀疑用户正在从事非法活动或是不适宜活动的时候，可以通过击键记录来必要收集一些证据。
- **恶意攻击者** 一个攻击者可以监视用户所有的击键行为，利用结果日志来提取口令、信用卡号以及其他种类的个人信息。这个击键监视器要求攻击者通过安装硬件设备或软件来攻破电脑，然后攻破系统获取信息。双因子认证方式减少了这种攻击成功的可能性。合适的物理安全和访问控制能减少击键监视的风险。另外，同样有必要对所有用户进行关于安全风险的培训。

14.8 常见 Windows 系统风险

所有的操作系统都存在安全风险。了解操作系统最常见的风险是十分重要的。大多数的攻击者就是通过扫描寻找存在漏洞的系统，从而对计算机进行攻击的。

SANS 研究所和 FBI 共同创建了 SANS/FBI 20 个最严重的互联网安全漏洞列表。这个列表包含了 Windows 和 UNIX 系统最常见的威胁。可以在 http://www.sans.org/top20/ 找到最新的列表。下面依据严重程度依次减弱的顺序列出了 Windows 系统最常见的漏洞。

（1）Internet Information Services（IIS）：微软的 Web 服务有多种不同的漏洞，包括处理异常请求和缓冲区溢出问题时的后门行为。IIS 安装之后常使用户和应用程序处于不受保护状态也是很常见的问题。除了 Windows 2003 之外，在 Windows 操作系统中 IIS 是被默认安装的。这种默认安装常造成管理者忽视安装细节。

（2）微软数据访问组件（MDAC）——远程数据服务：旧版本的 MDAC 包括一个漏洞，允许攻击者以管理员权限在本地运行命令。对于这种漏洞的攻击，用户的数据库是脆弱的。

（3）Microsoft SQL 服务器：MSQL 有几个常见漏洞使得攻击者能够访问数据库的内容。这些漏洞包括端口开放问题以及不安全的默认用户和不安全的试用应用程序问题。几种典型的恶意代码是以 MSQL 漏洞为目标的。

（4）NetBIOS——不受保护的 Windows 网络共享：Windows 提供了一种简单的方法使得远程计算机能够访问、共享本地的资源。这种特性通常是通过共享文件夹和共享打印机实现的。这种共享机制如果设置得不合适能够使得一个远程攻击者获得本地主机文件系统的全部控制。

（5）匿名登录——空会话（Null Sessions）：Windows 使用无用户 ID 的登录方式收集计算机的信息并执行一些连接服务。这种登录方式被叫做空会话（Null Sessions）。因为 Null Sessions 允许访问像用户或用户组账户和共享这样含有漏洞的信息，就为攻击者提供了极具吸引力的入侵点（entry point）。

（6）局域网管理员认证（LAN Manager Authentication）——Weak LM Hashing：Windows 支持局域网管理员认证，尽管只有很少的系统真正需要这种服务。局域网管理员相应的弱口令使得攻击者攻破任何存储的口令都是相当简单的。通过这个系统能够获得破解的口令。

（7）通用 Windows 认证（General Windows Authentication）——无口令账户或弱口令账户：令人震惊的是，许多系统居然有未设置口令的账户，而其他账户的口令则极容

易被攻破。

（8）因特网浏览器（IE）：万维网的流行使得和网络相关的攻击非常的流行。因为 IE 是上网最流行的接口，也就成为了网络攻击最常见的目标。这种产品有几种不同类型的安全漏洞，主要是针对它的高级功能和脚本功能。

（9）注册表远程访问：对于运行 Windows 操作系统的计算机，其中心数据库是注册表。注册表的任何更改都能够动态地改变系统的工作。不合适的安全设置能够使得远程用户修改关键的注册表设置。

（10）Windows Scripting Host（WSH）：WSH 使得运行 Windows 操作系统的计算机能够执行任意扩展名为.vbs 的文本文件。这种文件是 Visual Basic 脚本语言。通过 WSH 运行 Visual Basic 脚本，旧版本的 Windows 可能会受到攻击。许多恶意代码攻击就是利用这种漏洞，包括著名的“Love Bug”蠕虫。

理解系统的常见漏洞并且采取合适的保护措施是十分重要的。事实上，如果攻击者比用户对系统了解的还多，那么，用户的系统就极有可能成为受害主机，受到攻击者的攻击。

14.9 常见 UNIX 系统风险

SANS/FBI 20 个最严重的互联网安全漏洞列表同时包含 UNIX 系统最严重的漏洞。用户可以在 http://www.sans.org/top20/上找到最新的列表。以下是 UNIX 系统最常见的几种漏洞。

（1）远程过程调用（RPC）：RPC 使得一台计算机上的用户可以在另一台计算机上运行命令。并且，用户往往能够以根权限在目标计算机上运行命令。这就使得攻击者可以攻破旧版本的 PRC 软件，获得根权限，从而运行任何想要的软件。

（2）Apache 网络服务器：尽管大多数的安全专家认为 Apache Web 服务器比 IIS 要安全，但是仍然存在着漏洞，并且有可能被不安全的安装。事实上，它的高安全性常使管理者产生一种安全的错觉，因此忽视了基本的安全设置。

（3）安全外壳（SSH）：为了避免其他远程访问软件存在的诸多安全漏洞，大多数的管理者转向 SSH。尽管 SSH 比 RPC 安全性高很多，但是，仍然包含着很多的软件漏洞。如同 Apache 漏洞一样，攻击者明白表面上的高安全性使得许多管理者变得更懒惰了。

（4）简单网络管理协议（SNMP）：SNMP 被使用在网络中来监视远端网络设备。旧版本 SNMP 应用中存在的许多漏洞为网络攻击打开了后门。

（5）文件传输协议（FTP）：FTP 是用来传输文件最常见的一种方法。在认证过程和文件传输过程中同时存在着漏洞。FTP 以明文形式向服务器发送口令。应用嗅探器捕获网络数据包就能够读取口令。认证问题能够泄露用户的证书，软件漏洞可以使攻击者获得根权限。

（6）R-Services——可信关系：旧版本系统通常使用几种“R-Services”来获得远程计算机上的服务。这些服务包括远程外壳（Remote Shell，Rsh），远程复制（RCP），远程登录（RLOGIN），以及远程执行（REXEC）。这些服务使得可信关系忽略掉每次命令执行时的认证指令。这种信任使得攻击者冒充成为一个可信的计算机，不通过认证就获

得了更高的权限。

（7）打印机网络共享（LDP）：这个守护程序使得远程用户提交打印工作。存在的缓冲漏洞使得攻击者获得了根权限。

（8）Sendmail：邮件发送程序的流行使其成为一个常见攻击的目标。攻击者可以利用旧版本程序的漏洞来创造缓冲区溢出或使用其他的漏洞来发起一个电子邮件攻击。

（9）BIND/DNS：和邮件发送漏洞相似，旧版本的 BIND/DNS 可以使得攻击者利用软件中存在的漏洞发起各种类型的攻击。

（10）通用 UNIX 认证——无口令账户或弱口令账户：令人震惊的是，许多系统居然有未设置口令的账户，而其他账户的口令则极容易被攻破。

和 Windows 系统存在的漏洞一样，了解 UNIX 系统存在的常见漏洞并且采取合适的保护措施对于用户来说是非常重要的。不论用户使用哪一种操作系统，漏洞都是存在的并且必须处理掉。

14.10　操作系统扫描和系统标识

在计算机系统运行的过程中，对系统的当前状态进行评估是十分重要的。这可能仅是为了预防，也可能是作为调查研究的一部分。很多时候，查找和分析系统状态信息的数据是十分必要的。对数据进行识别、提取、记录，并从中搜集某些特殊活动证据的过程叫做计算机取证。这个过程包括提取日志文件以及文件系统中的内容，从而找到在系统中存在着哪些东西，以及用户已经做了哪些事情。

分析的目的是记录计算机的当前状态。这个信息可以用在之后的比较中，对于侦查一些不正常的行为以及系统性能的改变都是很有用。提取和记录系统的状态叫做系统标识。系统标识就是实时记录计算机在某一个固定时间点状态的一系列信息。系统设置、测试以及运行后都应该进行计算机标识的收集。随后再与之前的信息做比较，从而记录系统状态中的改变。

当怀疑一些不合适的或者非法的行为时，用户采取的第一步措施就是调查。调查中一个重要的组成部分就是提取日志文件和其他记录用户行为的数据。用户在计算机上几乎所有的活动都会被记录下来。这些活动日志提供了进行调查的合适的工具以及知识。系统取证是一门崭新的学科，被用在很多调查中来收集可疑行为的证据。第 13 章具体介绍了计算机取证的过程。

习　　题

一、选择题

1. 操作系统管理的主要系统资源不包括下列哪一项？（　　）

A. 主存储器

B. 二级存储器

C. 三级存储器

D. 处理器

2. 一个系统使用击键监视器的原因不包括下列哪一项？（　　）

A. 系统备份

B. 恶意攻击

C. 证据收集

D. 测试和质量保证

二、问答题

1. 简述操作系统安全的特点和好处。

2. 简述系统备份的重要性和危险。

3. 思考如何实现 Windows 和 UNIX 最基本的安全设计。

课后实践与思考

常用操作系统扫描工具介绍及操作示范

1. CIS-CAT

- **功能** 可以根据不同的操作系统，选择不同的基准进行系统漏洞扫描。
- **适用对象** UNIX/Linux、MS Windows，并且这些系统上装了 java 5 或以上版本。

本文主要介绍在 Linux 操作系统下的用法。

（1）扫描准备

将工具解压到目标 Linux 机器上，CIS-CAT 扫描 Linux 机器必须要求机器安装 JDK 在 1.5 或以上可以通过#java -version 查看具体的版本号，如果机器上有 JDK 在 1.5 以上但是只是没有设置环境变量，参照以下方法设置，如果没有版本在 1.5 或者以上，则下载 1.5 或者以上版本安装。

更新环境变量参照如下：

```
#vi .profile

PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:$HOME/bin:/usr/X11:/sbin:/bin:/usr/local/bin:/i2kmount/iToolcfg/icheck/jdk1.5/jre/bin:/i2kmount/iToolcfg/icheck/jdk1.5/bin:.

export PATH

JAVA_HOME=/i2kmount/iToolcfg/icheck/jdk1.5

export JAVA_HOME
```

（2）扫描执行

具体扫描执行命令如下：

```
#./CIS-CAT.sh ./benchmarks/suse-10-benchmark.xml  //根据具体扫描系统，确定后面的基准参数
```

（3）扫描结果

扫描结果存放在当前用户根目录下的 CIS-CAT_Results 文件夹里。

2. SRay（SRay.0.4.8.tar.gz ）

- **功能** 系统漏洞扫描。
- **适用对象** UNIX/Linux 系统。

这里用 SRay 来扫描 Linux 系统。

（1）扫描准备

将 SRay.0.4.8.tar.gz 工具解压到目标 Linux 上。

（2）扫描执行

具体扫描执行命令如下。

```
Linux Security Config Test Task Information

Test Date: Mon Jun 29 07:51:32 2009

User Name [Tester]:                        //默认即可，直接按 Enter 键

Target Product Name [88]:                  //默认即可，直接按 Enter 键

Target Product Version [66]:               //默认即可，直接按 Enter 键

----------------------------------------------------

----------------------------------------------------

If you input 'Y' or 'y', you must answer several qu-

estions regarding the security configuration of your

system.

Reference information is available for only some of

these questions.

If you simply press 'Enter' key or input 'N' or 'n',

the manual and semi-automatic test items will be sk-

ipped and these items' results will use the previous

test results （i.e.,new test results will not be gen-

erated)

Before you select,please read the above notice!

Execute manual or semi-automatic test item（s）?

Yes （Y/y） or No （N/n）?

Y                                          //选择 y，自动测试
```

（3）扫描结果

扫描结果存放在当前执行目录下的 Result 文件夹里。

3. Nessus

- **功能** 检查系统存在有待加强的弱点，电信运营商、IT 公司、各类安全机构也普遍认可该工具的权威性，通常都会使用它作为安全基线扫描工具。
- **适用对象** UNIX/Linux，MS Windows。

本文主要介绍 Nessus 安装在 Windows 系统下的用法。

（1）扫描准备

将 Nessus 安装在一 Windows 机器上，使用 Nessus-3[1].2.1.1 版本，不用注册码。

由于是 C/S 模式，客户端要连接服务器扫描，在客户端连接服务端时，此版本服务端的 IP 只能设成 127.0.0.1，才可以连接成功。

（2）扫描执行

扫描 Linux 机器必须设置 ssh 用户名密码（如下），其他默认设置。

扫描 Windows 机器必须设置 ssh 用户名密码，其他默认设置。

（3）扫描结果

扫描完后，只需在 REPORT 标签项将结果导出指定目录下就可以了。

4. MBSA

- **功能** 微软免费提供的安全检测工具，Microsoft 基准安全分析器（Microsoft Baseline Security Analyzer，MBSA）是微软公司整个安全部署方案中的一种，它目前的主要版本是 v1.2.1。该工具允许用户扫描一台或多台基于 Windows 的计算机，以发现常见的安全方面的配置错误。MBSA 将扫描基于 Windows 的计算机，并检查操作系统和已安装的其他组件（如 IIS 和 SQL Server），以发现安全方面的配置错误，并及时通过推荐的安全更新进行修补。
- **适用对象** MBSA V1.2 能够扫描运行以下系统的计算机：Windows NT4、Windows 2000、Windows XP Professional、Windows XP Home Edition 和 Windows Server 2003。MBSA 能够从运行以下系统的任何一台计算机上执行：Windows 2000 Professional、Windows 2000 Server、Windows XP Home、Windows XP Professional 或 Windows Server 2003。Windows 系统扫描，MBSA 不像 SUS 之类的产品那样丰富和全面，但却能够迅速地找出系统存在的安全隐患，特别适合个人用户和小型网络环境（如对等网络）使用。

本文介绍 MBSA 扫描 Windows 系统。

（1）扫描准备

将 MBSA 安装在要扫描的 Windows 机器上，使用版本可以为 MBSASetup-x86-EN.msi。

（2）扫描执行

MBSA 每次运行时都会尝试从微软网站下载一个 mssecure.cab 文件，这是一个压缩的 XML 文件，它列出了所有最近的更新。如果本地网络上有 SUS 服务器，MBSA 可以配制成从 SUS 下载的 mssecure.cab 文件（而不是从微软下载）——当然，MBSA 只能根据它所使用的 mssecure.cab 文件报告尚未安装的更新。

执行全面的MBSA扫描需要目标系统上的管理员权限。如图 14-4 所示，运行 mbsa.exe

启动 MBSA 的图形界面的版本，图形界面的优点是简单易用，可以直观地设置要扫描的计算机和扫描类型。设置扫描目标的方法是单击 Pick a computer to scan 或 Pick multiple computers to scan 按钮，输入一个 IP 地址、一个 IP 地址范围或一个域名。

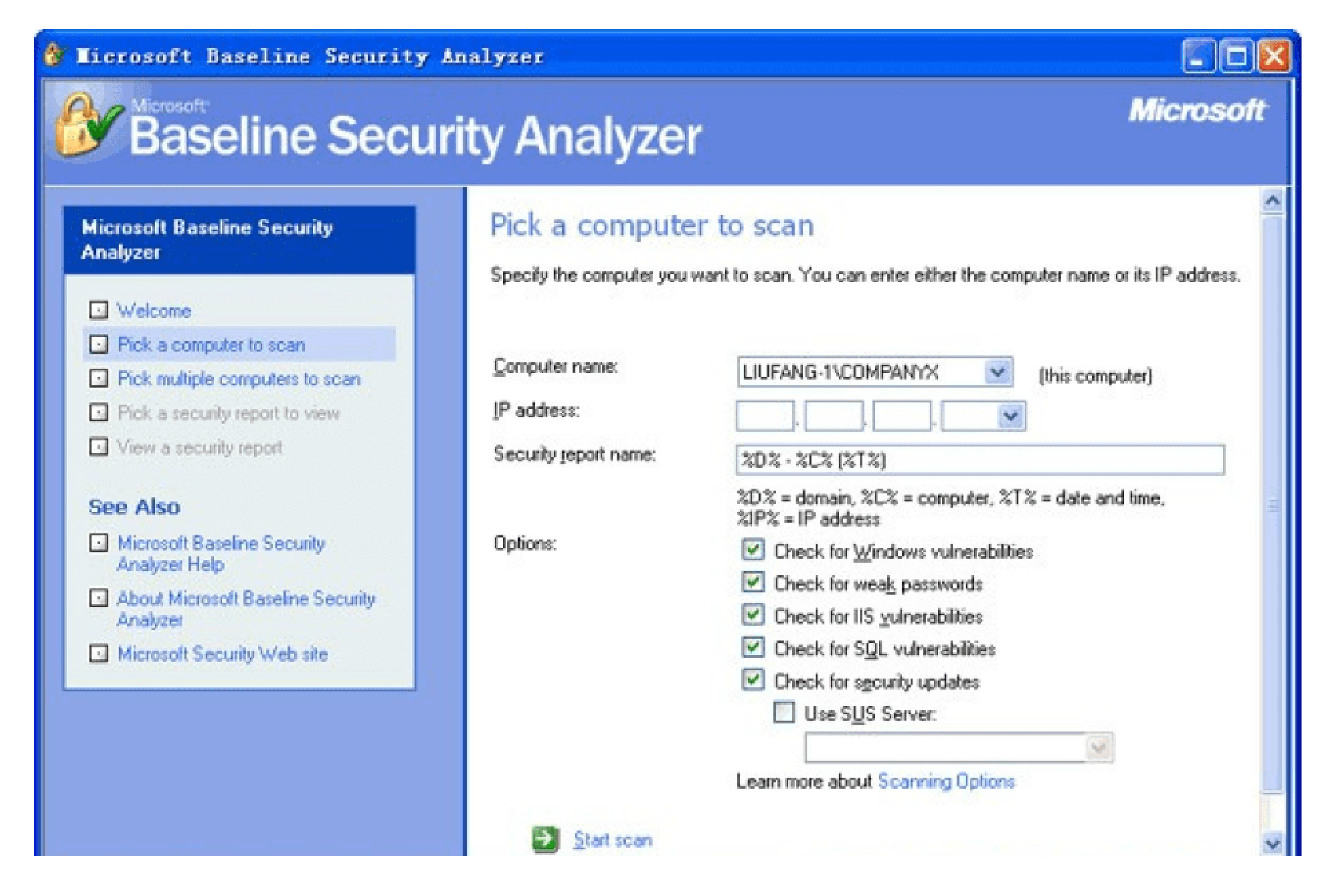


图 14-4　设置扫描目标

其次是设置扫描选项，例如检查 Windows 漏洞等，另外还可以指定一个 SUS 服务器，让 MBSA 从 SUS 服务器下载一个软件更新的清单与各目标机器比较；如不指定 SUS 服务器，MBSA 将从微软网站下载软件更新的清单。默认情况下，图形界面的 MBSA 将执行微软所谓的“基线扫描”，即只扫描和报告 Windows Update 定义的“关键更新”，而不是扫描和报告所有的安全更新。

在图 14-4 中，单击 Start scan 按钮开始扫描。扫描所需的时间与具体的扫描项目和机器数量有关。

MBSA 可以选择要扫描的计算机包括如下。

❑ **单台计算机**

MBSA 最简单的运行模式是扫描单台计算机，典型情况表现为“自动扫描”。当选择“选取一台计算机进行扫描”时，可以选择输入想对其进行扫描的计算机的名称或 IP 地址。默认情况下，当用户选中此选项时，所显示的计算机名将是运行该工具的本地计算机。

❑ **多台计算机**

如果用户选择“选取多台计算机进行扫描”时，将有机会扫描多台计算机，还可以选择通过输入域名扫描整个域，还可以指定一个 IP 地址范围并扫描该范围内的所有基于 Windows 的计算机。

如要扫描一台计算机，需要管理员访问权。在进行“自动扫描”时，用来运行 MBSA

的账户也必须是管理员或者是本地管理员组的一个成员。当要扫描多台计算机时，必须是每一台计算机的管理员或者是一名域管理员。

扫描类型包括以下几种。

❑ **MBSA 典型扫描**

MBSA 典型扫描将执行扫描并且将结果保存在单独的 XML 文件中，这样就可以在 MBSA GUI 中进行查看（这与 MBS AV1.1.1 一样）。可以通过 MBSA GUI 接口（mbsa.exe）或 MBSA 命令行接口（mbsacli.exe）进行 MBSA 典型扫描。这些扫描包括全套可用的 Windows、IIS、SQL 和安全更新检查。

每次执行 MBSA 典型扫描时，都会为每一台接受扫描的计算机生成一个安全报告，并保存正在运行 MBSA 的计算机中。这些报告的位置将显示在屏幕顶端（存储在用户配置文件文件夹中）。安全报告以 XML 格式保存。

用户可以轻松地按照计算机名、扫描日期、IP 地址或安全评估对这些报告进行排序。此功能能够轻松地将一段时间内的安全扫描加以比较。

❑ **HFNetChk 典型扫描**

HFNetChk 典型扫描将只检查缺少的安全更新，并以文本的形式将扫描结果显示在命令行窗口中，这与以前独立版本的 HFNetChk 处理方法是一样的。这种类型的扫描可以通过带有“/hf”开关参数（指示 MBSA 工具引擎进行 HFNetChk 扫描）的 mbsacli.exe 来执行。注意，可以在 Windows NT 4.0 计算机上本地执行这种类型的扫描。

❑ **网络扫描**

MBSA 可以从中央计算机同时对多达 10 000 台计算机进行远程扫描（假定系统要求与自述文件中列出的一样）。MBSA 被设计为通过在每台所扫描的计算机上拥有本地管理权限的账户，在域中运行。

在防火墙或过滤路由器将两个网络分开的多域环境中（两个单独的 Active Directory 域），TCP 的 139 端口和 445 端口以及 UDP 的 137 端口和 138 端口必须开放，以便 MBSA 连接和验证所要扫描的远程网络。

（3）扫描结果

扫描的结果默认存在 C:\Documents and Settings\Administrator\SecurityScans 目录下，每一台计算机分别有一个独立的 XML 格式的报告，每个报告文件的体积约为 20 KB。

扫描结束后，单击 Pick a security report to view 按钮并查看安全报告。MBSA 允许按计算机名称、IP 地址、扫描日期排序报告文件，不过几遍扫描下来，文件夹里面仍会堆积起大量的文件，所以最好及时删除过时的报告。

如果是第一次用 MBSA 扫描网络，很可能得到一份让人大吃一惊的报告——新安装的系统，无论是 Win 2000 还是 XP，都无法通过 MBSA 的扫描检查。

MBSA 不能提供综合性的报告，所有报告都是针对单台机器的。单击一台计算机的名称，MBSA 显示出这台机器的安全漏洞和未安装补丁的摘要报告，如图 14-5 所示。

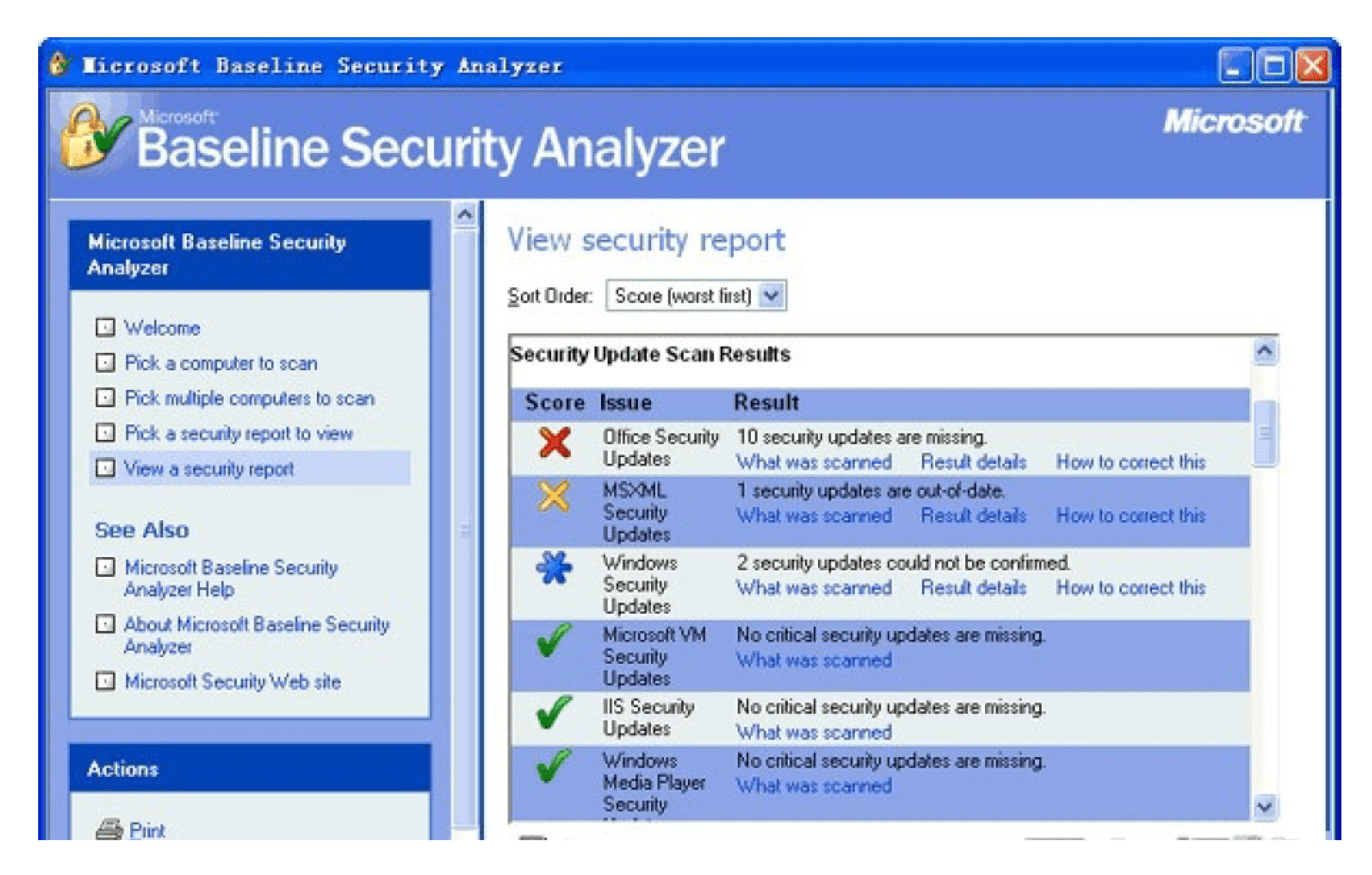


图 14-5　单机报告

对于大多数发现的问题，MBSA 会提供进一步的详细资料。例如，假设 MBSA 报告 Password Expiration（密码过期）检测没有通过，单击 Result details 按钮可以看到哪一个账户的密码被设置为永不过期。另外，What was scanned 和 How to correct this 提供了直接指向 MBSA 帮助文件的链接，详细解释已经发现的问题及解决办法。

MBSA 的摘要报告分 5 个部分，即 Security Update Scan Results（安全更新扫描结果）、Windows Scan Results（Windows 扫描结果）、Internet Information Services Scan Results（IIS 扫描结果）、SQL Server Scan Results（SQL Server 扫描结果）以及 Desktop Application Scan Results（桌面应用程序扫描结果）。例如，在 Windows Scan Results 中，MBSA 将非 NTFS 分区和启用 GUEST 账户视为安全隐患，将具体的审核设置、服务状态和共享资源当作附加信息。MBSA 将报告被扫描机器的所有共享资源，包括共享级别以及目录的 ACL 设置。

综上所述，虽然 MBSA 不像 SUS 之类的产品那样丰富和全面，但却能够迅速地找出系统存在的安全隐患，特别适合个人用户和小型网络环境（如对等网络）使用。

第 15 章　操作系统加固

本章学习重点：

- 操作系统加固的概念
- 安全操作系统必要的组成部分
- 安全检查列表的重要性
- 操作系统特定的安全特性
- 基本的文件系统安全

通过对大量的操作系统进行分析发现，操作系统存在大量的安全漏洞。另外，相关数据表明简单但高效的安全实践能够有效地阻止对系统攻击。目前，已经产生了一些基本原则来维护系统的安全。应用有效的安全实践，能够减少大量导致个人或企业损失的安全风险。

管理员必须了解系统最常见的威胁，并且能够对系统安全策略进行审查以确保解决这些安全威胁。本章讨论了对操作系统进行加固的必须步骤，包括保证操作系统安全的基本策略，以及把这些规则形式化为适用于 Windows 系统和 UNIX 系统的安全检查列表。

15.1　操作系统加固的原则和做法

构建安全系统的第一步就是要创建一个完整全面的安全策略，当然，可靠的安全策略仅是一个起点。根据安全策略的安全实践对系统实施安全控制，用户必须根据策略的建议实施安全行为，以保证采取的安全控制是适当高效的，这是一项花费时间和资源的任务。要确保软件保持最新版本，并且保证所有已知的安全漏洞都已被关闭是件很不容易的事情。事实上，仅是了解哪些是严重的安全漏洞就已经很不容易了。用户需要建立一个明确的规则来检查和更新软件、硬件以及安全策略；为不同的用户分配任务；设置时间表。其实，基本的主动防御就能够阻止大量的安全违规行为。

用户的总体目标就是加固系统，也就是采取措施使系统更加安全。操作系统加固包括许多任务，如在封闭的计算机机房中保存敏感的服务器，构建复杂的口令策略，以及监视网络的登录情况。加固系统是一个反复进行并且不断变化的过程，需要耐心和恒心。加固结果使系统能够抵抗攻击，并且保护系统内部的数据。为了实现这个目的，用户需要首先评估系统当前的安全水平，然后执行必要的调整，并且对这些改变进行测试，之后，需要不断重复这些步骤。

用户加固的过程也要从最初的安全策略开始。首先应该识别系统的威胁，然后选择合适的安全控制手段。用户在执行了一次安全控制的全过程之后，对安全策略进行完整性和有效性检查应该是一项简单的任务。但是，不要偷懒，为系统维持有效的安全策略是非常重要的，安全策略一旦过时，也就失去了保证系统安全的能力。

15.2 操作系统安全维护

保持系统安全是风险非常高的一件事情。用户必须处于系统攻击者的前面。系统攻击者可以试图在未授权的情况下访问计算机的任何人。访问系统时，攻击者常有恶意企图。许多人使用黑客一词来指代攻击者。真正的黑客通常并不具有恶意企图，而只是享受编程过程中的学习乐趣。然而，攻击者和黑客经常交换使用。用户的目标是避免成为受害者。攻击者之间常共享系统漏洞并分享经验。一旦攻击者利用一个新的系统漏洞进行攻击，这个方法就会出现在取证报告中。有关新漏洞的消息就成为了焦点，经过一段时间之后，硬件或软件的制造者就会发布一些补丁来减少问题，之后相关的攻击就会变少。

用户系统最可能被攻击的时间是在新漏洞被发现后不久。对新出现的漏洞及其应对措施保持更新是非常重要的。有些时候尽管用户不能把自己的系统变得牢固不可攻破，但可以使攻击者对自己的系统失去兴趣。攻击者很可能放弃你的系统去而去寻找一个更加容易的目标。

为了保持对新出现威胁的更新，其最基本的步骤是保证操作系统以及软件是最新版的。用户要咨询操作系统供应商以及系统的所有重要软件的提供者来了解如何保持更新。

尽管补丁的绝对数量可能很大，但是在安装补丁之前要确保已经理解了补丁的功能。在安装新的软件之前，同样要确保拥有有效的系统备份。因为有些时候，用户安装的补丁可能会导致系统不可用。在这种情况下，一个直接的恢复途径是非常重要的，这就需要有一个当前的系统备份。要记录下已经在系统中安装的软件，并且保持更新。攻击者对系统进行扫描，看到最新更新的软件时，可能会放弃攻击这个用户。

15.3 安装安全检查软件

对系统进行加固的最好的方法之一就是使用安全检查列表。要记住关闭系统中所有安全漏洞所必须的步骤是不可能的。安全检查列表能够随时跟踪用户的行为，避免用户忘记重要的系统检查和修改。用户在进行一项重要工作的时候，也需要使用安全检查列表，这能简化任务。

安全检查列表的产生方式决定了它的效力。一个好的检查列表是根据大量的经验以及安全专家的意见形成的。这个列表应该是过去保护计算机安全的所有方法的总结，包括已经采取的措施以及还没有采取的措施。当系统安全非常重要的时候，用户可以应用一个在安全环境中开发和测试的检查列表。用户完成每一个步骤之后，要花一些时间记录下工作进展，并做一些适当的标记。用户需要对检查列表不断进行更新，以反映出最新的信息和经验。随着系统和软件的不断改变，保证信息安全所需要的步骤也应该不断地更新。

对于检查列表，每一个操作系统都有不同的行为条目，尽管这其中的许多概念都是相同的，用户也会发现对于不同的系统功能也需要不同的检查列表。用户在保护 Web 服务器安全所采取的措施和保护数据库服务器安全所采取的措施很可能是不一样的。尽管

操作系统可能是相同的，但是对于两种不同类型的计算机用户很可能会使用不同的软件和访问请求。用户需要创建和维护所需的不同检查列表，但要注意不能创建得太多。一个好的检查列表要不断地成熟，拥有太多的检查列表会使得系统维护变得异常困难。

创建安全检查列表的第一步是要创建一个标准列表。用户可以在操作系统供应商的Web 站点上查询安全检查列表，同时也要访问其他提供系统管理策略的 Web 站点。使用标准列表作为一个起点，然后根据自己的环境对这些规则进行改进。下面的部分列出了Windows 和 UNIX 系统的一些基本的行为条目。这些只是起点，用户还需要将自定义项目加载到列表中。

15.3.1 Windows 安全检查列表

对计算机进行保护就是实施一系列的行为，避免可能伤害到系统或系统支持的数据的行为发生，这是一个概括的叙述。如果用户在组织中使用多种操作系统，就需要分别关注每一种操作系统的特殊需要。首先讲述 Windows 操作系统的安全检查列表，它由 4 个基本方面组成。

1. 加固 Windows 注册表

Windows 操作系统中，注册表是系统信息的中心存储库。操作系统的任何操作都需要使用注册表这个数据库。注册表的值存储在注册表键值（registry keys）中，它们是以树型层次结构管理的。如果想要修改注册表的键值，在 Windows 桌面选择“开始”→“运行”命令，在打开的文本框中输入“regedit.exe”或“regedt32.exe”，单击 OK 按钮，Windows 注册表编辑器就打开了。当然还有其他第三方的应用程序可以用来编辑注册表。

在微软的网页 http://www.winguides.com/registry/上可以看到更多关于注册表的信息。

表 15-1 列出了加固 Windows 时需要考虑的一些 Windows 注册表的键值。

表 15-1　和安全相关的常见 Windows 注册表键值

功能描述	键值名称
阻止访问特定驱动器的内容	NoViewOnDrive
限制用户能够运行的应用程序	RestrictRun
关闭注册表编辑工具	DisableRegistryTools
关闭关机（shutdown）命令	NoClose
关闭 Windows 热键	NoWinKeys
限制对 Windows 升级特性的访问	NoWindowsUpdate
管理系统策略升级	UpdateMode， NetworkPath，Verbose，Load Balance
限制更改用户文件夹位置	DisablePersonalDirChange，DisableMy PicturesDirChange， DisableMyMusic-DirChange，DisableFavoritesDirChange
应用基于用户的定制外壳	Shell

仔细研究表 15-1 列出的数值，然后为系统选择最合适的值。同样可以向微软网站以及其他 Windows 相关的站点来咨询关于 Windows 注册表的更深层次的内容。另外，在 Windows XP 系统中，用户可以为每个 Windows 注册表键值赋予 11 个权限。对于每个键值，单击，然后选择权限，可以为每个键值设定权限，完成键创建，子键创建、键删除，以及 8 种其他权限。可以为受保护的键值设定明确的键值权限，以避免未授权的更改。

2. 删除不必要的服务

Windows 操作系统的默认安装设置为用户提供了很多精心制作的功能，但使用这些功能也要花费一定的代价。这些附加功能的运行会浪费宝贵的 CPU 资源，并且给攻击者提供了入侵系统的机会。简而言之，附加的服务提供了更多的系统登录点。加固操作系统，用户要确保已经关闭了那些不必要的服务。表 15-2 列出了几种用户系统可能不需要的常见服务。

表 15-2　Windows 系统中用户可能不需要的几种服务

服务名称	功能描述	注释
文件共享	允许远程用户访问本地磁盘和文件	关闭此项服务
打印机共享	允许远程用户是用本地打印机打印	关闭此项服务
Internet 信息服务（IIS）	微软的 Web 服务器	除非管理一个 Web 站点，否则不要安装此项服务
网络会议远程桌面共享（NetMeeting Remote Desktop Sharing）	允许他人共享桌面	除非需要，否则关闭该服务
远程桌面帮助会话管理员（Remote Desktop Help Session Manager）	允许运程支持	除非需要执行远程支持，否则关闭该服务
远程注册	允许远程用户修改和维护注册表	如果不打算远程管理注册表，关闭该服务
路由和远程访问（Routing and Remote ）	允许对系统的远程访问	除非需要拨号访问系统，否则关闭该服务
SSDP 目录服务（SSDP Discovery Service）	支持普遍的 PnP 服务	关闭该服务，关闭 5000 号端口
Universal Plug and Play Device Host	允许系统连接到网络上可用的设备	关闭该服务
远程登录	允许远程用户登录到系统上	因为所有的信息，包括口令都是以明文方式传递的，关闭该服务，使用 SSH

3. 网络协议和网络服务加固

对于那些不能关闭的剩余服务，用户要尽量限制对其进行访问。下面列出了用户需要处理的一些方面。

（1）使用防火墙。用户可以使用硬件防火墙或者是软件防火墙。硬件防火墙可以在任何时候保护用户，软件防火墙只能在软件运行的时候对用户进行保护。如果用户的系统连接在互联网上，要保证防火墙是开启的。同时，要确保防火墙是合理设置的。

（2）关闭所有不需要的网络协议。

（3）对所有和远程访问以及远程联网相关的服务进行检查，考察是否真正需要每一项服务。对于自己不能识别的服务，可以咨询微软的网站以获得另外的信息。用户在做任何更改之前，先创建一个系统基线。如果用户对系统进行的改变引起了负面作用，就可以返回到基线。

4．对系统服务、设置和文件进行加固

除了之前所讨论的这些措施，下面给出了另外一些用户不能忽视的部分。

（1）保证计算机的物理安全。采取措施保证没有权限的人远离计算机，尤其是服务器。

（2）及时更新 Windows 操作系统的补丁。微软通过 Email 或直接的系统信息向用户提供及时的更新通知。访问微软的 http://windowsupdate.microsoft.com 网页，获得更多的信息。

（3）使用 Microsoft Baseline Security Analyzer（MBSA）来对系统安全进行评估。访问站点 http://www.microsoft.com，找到 HFNetChk，下载、安装并且运行这个应用程序。用户很可能还需要下载并安装额外的补丁。

（4）在日常使用时，不要设置管理员账户，为每一个用户设置单独的用户账户。

（5）关闭 guest 账户。

（6）确保所有用户使用口令，并且保证一个口令都遵循强口令策略。实施强口令的一种方法就是定期地在电脑上运行口令破解程序。

（7）在系统上安装反病毒软件包。执行全面的系统病毒扫描并确保完全的病毒防御功能。确保软件以及签名数据库是最新版本的。在更新之后，立即运行全面的系统扫描。

（8）确保所有的备份介质是受保护的，远离破坏和偷盗。

（9）为 Windows XP 系统运行加密文件系统。

（10）运行系统审计功能。

（11）关闭 CD-ROM 自动运行功能。

15.3.2 UNIX 安全检查列表

加固 UNIX 系统时考虑的因素和加固 Windows 系统时考虑的因素是很相似的。尽管理念类似，但两个系统之间还是存在本质区别，所以需要在每一种环境中针对每一种不同的系统做单独的讨论。下面，讨论在加固 UNIX 系统时，用户必须处理的一些方面。

1．删除不必要的 UNIX 协议和服务

和其他操作系统一样，用户应该关闭所有不必要的协议和服务。表 15-3 列出 UNIX 系统不常用的服务和守护进程。为了获得最大的系统安全，需要将这些程序关闭，只在

用户真正需要的时候再开启。这种方法会花费一些时间，但是用户却能找到自己真正需要的服务。对于从守护进程 inet.d 开始的服务，需要编辑/etc/inet.d 文件。在每一行开始的地方加一个“#”标志，就能阻止这个命令行所描述的服务在系统启动的时候运行。

表 15-3　UNIX 系统中用户不需要的几种服务

服务名称	功能描述	注释
远程访问（Telnetd）	允许远程用户访问	关闭该守护进程，使用 SSH
Fingerd	提供系统上用户的相关信息	除非是必须的，关闭该守护进程
R-commands （rlogin，rsh，rcp，...）	允许远程用户和系统进行交互作用	关闭该命令
Cron	在指定时间执行命令	拒绝普通用户的 Cron
RPC	远程过程调用	如果不是必须的，关闭该服务
Ftpd	使用文件传输协议（FTP）传输文件	如果不需要提供 FTP 访问，关闭该服务
TFTP	使用 FTP 简单版本传输文件	关闭该程序
UNIX to UNIX copy（UUCP）	传输文件	关闭该服务
Sendmail	发送以及运送电子邮件	除非需要处理电子邮件，否则关闭该服务。需要处理电子邮件时，考虑其他方法
NFS，SAMBA，AFS，DFS	提供对文件和内存的网络访问	除非必须，否则关闭该服务

2. 使用 TCPWrapper

攻击者用来和目标系统进行通信最常用的协议就是 TCP 协议。不幸的是，这也是所有其他人最常使用的协议。关闭所有 TCP 通信能够使系统更安全，但同时也会使系统无法在正常情况下通信。有一种方法能够使用户获得更好的 TCP 安全而又不必放弃 TCP 功能。一个好的防火墙能够把许多通信在到达用户系统之前过滤掉。但是，用户仍然需要检查通过防火墙的数据包。TCPWrapper 包给了用户进一步过滤通信以及记录可疑行为的能力。

TCPWrapper 是 tcpd 守护进程更常见的名字，用来拦截和检查所有的 TCP 通信并决定接受还是拒绝每一个请求。TCPWrapper 对发送方的 IP 地址进行双向（double-reverse）查找来寻找欺骗地址。如果 DNS 的记录和请求数据包中的 IP 地址不一致，这个请求就会被拒绝，并被记录为一个失败的链接请求。如果这两个地址一致，TCPWrapper 就将源主机名以及被请求的服务和访问控制列表进行比较来决定是否允许请求。如果到这一步时，没有出现异常，这个请求就会被记录下来，同时可能会运行一个可选的程序，这个请求被通过并且到达“真正的”守护进程。

TCPWrapper 能够截获所有的 TCP 通信，并且在数据包通往另一个守护程序之前，它能根据一系列的行动进行裁决。不论何种原因，如果请求是可疑的，守护程序就会够终止这个请求，并记录这个可疑行为，还很可能运行一个程序提醒管理员，并且把此请求归档备份用来进行之后的调查。需要注意的是，任何的过滤机制都会产生负面作用。对于每一个可疑的请求，要仔细考虑是否应该发送一个警告。管理这类请求的一个更好的方法就是经常检查 TCPWrapper 产生的日志文件。

3. UNIX 系统的其他安全措施

除了之前所给出的这些措施，还应该实施以下这些措施。

（1）保证计算机的物理安全。采取措施保证没有权限的人远离计算机，尤其是服务器。

（2）保证操作系统补丁及时更新。操作系统供应商的网站会有最近更新的信息。

（3）要保护高级用户的 ID，只在必须的时候使用它们。为每一个访问系统的用户创建新的用户账户，关闭无用的账户。

（4）确保所有用户都使用口令，并且遵循强口令策略。定期运行口令破解程序。

（5）安装防病毒软件补丁，执行全面的系统病毒扫描，运行彻底的病毒防范功能。保证软件以及签名数据库保持更新。在任何升级之后，立即运行全面的系统扫描。确保所有的备份介质受到保护，远离破坏和偷盗。

（6）执行系统审计，定期查看审计日志。

（7）运行漏洞扫描程序。

15.4 文件系统安全

操作系统安全中最重要的方面就是用户必须保证文件系统的安全。操作系统的文件系统是一系列在次级存储设备（secondary storage devices）上用于管理、存储数据和文件的程序。文件系统软件使得用户可以将数据存储在硬盘上，在使用的时候再将数据取回来。为了方便查找文件，文件系统使用目录或文件夹的树形结构进行管理。当然，存储介质也不仅局限于硬盘。文件系统不仅处理文件访问请求，而且还处理访问控制。

UNIX 和 Windows 文件系统都使用树形结构来管理文件。树的访问节点（Entry Point）叫做根目录。一台计算机可能有很多的磁盘，每个磁盘能够被分为几个部分，叫做分区。每一个磁盘分区通常有一个独立的文件系统和自己的根目录。在 Windows 中，每一个文件系统有自己的驱动器号（A～Z）；每一个 UNIX 文件系统有一个载入点。

从安全角度讲，用户了解操作系统如何处理安全是十分重要的。每一个目录和文件有着独立的权限，规定着哪个用户可以浏览和修改文件系统。下面 3 个部分包含了有关文件系统的问题。

1. NT 文件系统安全（NTFS）

Windows 服务器首选的文件系统是 NT 文件系统（NTFS）。比起 FAT 文件系统，NT 系统更新也更安全。NTFS 是随着 Windows NT 制造出来的，并且已经被增加到 Windows 的更新的版本中。NTFS 能够在多用户环境中为文件和文件夹提供更多的保护。

NTFS 安全的核心是访问控制列表（ACL）。每个文件或文件夹客体实际上有两个相应的 ACLs，为了简便，只考虑有一个的情况。在 Windows NT、Windows 2000 以及 Windows XP 中，每一个文件或文件夹客体有 6 种相应的权限。表 15-4 列出了 NTFS 在 Windows NT/2000/XP 中存在的基本权限。

表 15-4　NTFS 的基本权限

权限名称	对文件的权限	对文件夹的权限
读（R）	读取文件内容	读取文件夹内容
写（W）	修改文件内容	修改文件夹内容
执行（X）	执行程序文件	Traverse a folder or subfolder
删除（D）	删除文件	删除文件夹
更改权限（P）	更改文件的权限设置	更改文件夹的权限设置
获得所有权（O）	取消文件所有权	取消文件所有权

Windows 2000 和更新的 Windows 操作系统版本使得管理员对文件和文件夹有更多的控制，用户可以获得 13 种不同的权限类型。每一个权限设置都被保存在一个访问控制目录（ACE）中。对被授权访问文件或文件夹的用户或用户组，都有一个单独的 ACE。事实上，一个客体可能有几个包含着权限信息的用户或用户组 ACE。当一个用户请求访问文件或文件夹客体的时候，用户 ID 和组关系就会和被请求客体 ACE 中的信息做比较。根据存储在 ACE 中的信息，操作系统授权或撤销对客体的访问请求。NTFS 使得管理员可以为系统中的每一个文件和文件夹提供非常明确的访问规则。

2. Windows 共享安全

Windows 操作系统支持文件夹和打印机的共享或远程使用。为了实现这个目标，在系统设置中，文件夹共享和打印机共享必须是打开的（Windows 95、Windows 98、Windows NT、Windows 2000、Windows XP 中文件共享和打印机共享的开放是默认的）。对每一个共享，用户可以自己明确不同的安全水平，即全局水平、共享水平以及用户水平。全局水平意味着每一个人都能够访问共享，共享水平意味着用户必须输入一个口令才能获得共享，用户水平意味着限制着某些用户的访问。当使用用户水平的安全设置时，用户为每一个用户和文件建立访问控制列表来存储访问权限。记住，一旦共享了一个打印机或文件夹，这个打印机或文件夹就能够被远程用户所访问，这具有一定的风险。

3. UNIX 文件系统安全

UNIX 文件系统使用的权限架构在某些方面很像 NTFS。事实上，应该说 NTFS 的方法在某些方面很像 UNIX 的权限设置，因为 UNIX 比 Windows 早产生很多年。之前已经介绍了文件模式设置。UNIX 系统中，每一个文件的权限包括读、写和执行。对于文件的所有者、组成员以及其他人有着不同的权限设置。这种方法似乎有些灵活，但是并不支持 NTFS 模式的权限继承。

在 UNIX 中，系统的所有权限都是明确的。远程用户必须出示身份证书才能获得对资源的访问权限。这点同 Windows 网络中经常应用的域（domain）的概念是不同的。尽管在 UNIX 系统中，基于文件的权限是本地（native）的，对 UNIX 文件系统安全模式进行扩展并且应用更加成熟的安全模式还是有可能的。但在试图使用另一层软件来加固文件系统的时候，需要花一些时间来真正理解 UNIX 系统的安全，而这些时间是很值得花费的。

15.5 操作系统用户管理安全

对于大多数的现代操作系统，最主要的访问请求是通过用户账户来完成的。一个潜在的用户会出示证书取得目标系统的识别和认证。一旦认证成功，根据存储在用户账户数据中的规则，就会授给用户一定的访问权限。这些规则的性质和形式可能非常广泛，但概念是相同的。用户登录进入系统，然后被授予一定的权利。

在任何一个操作系统中，和用户账户相关的最常见的漏洞就是弱口令。尽管之前也提到过这个问题，但还需要重复一下：一定不要使用弱口令！建立一个强口令政策，然后执行。必须不断教育和提醒用户，使他们意识到自己对系统安全的义务。要向系统的用户解释一个好的口令规则是多么的重要。运行了强口令之后，要运行一个口令破解程序来检查口令的强度。有很多口令是可以被猜到的，其数量往往多得令人惊奇。

因此，一个强口令是什么样的呢？要如何指导系统的用户运用强口令呢？这里是一些简单的规则：口令要难于被猜测，不要使用个人信息，不要重复口令，不要把口令写下来，定期对口令进行更新，使用大小写字母、数字、和标点符号来构造口令。

了解了创建口令的方法，来看看一些 Windows 和 UNIX 系统的账户安全策略。

15.5.1 Windows 账户安全策略

尽管可以在 Windows 中创建本地用户，但最常见的安全策略是在域层次创建用户。如果正在运行 Windows NT、Windows 2000，或其他更新的 Windows 操作系统版本，域控制器安全模式使得安全权限更集中。作为一个用户，可以登录到域中的任何一台计算机，并且保持自己的访问权限。定义一个用户的过程是简单的，只需要在域控制器计算机上添加一个用户。只有拥有管理员权限才能创建用户。一旦已经创建了一个或多个用户，可以创建安全用户组，并且可以把用户放在一个或多个组中。通过工作组分配权限，可以使权限管理过程变得简单。比起给 6 个或 60 个个人用户分配对数据库文件夹的写权限，给 DBA 这个组分配同样的权限要简单得多。在开始运行用户账户之前要做一个用户账户的安全计划。在长时间的运行中，提前考虑所请求的用户、工作组及用户和工作组的权限会节省很多的时间。

15.5.2 UNIX 账户安全策略

和 Windows 系统一样，在 UNIX 中有两种类型的账户——用户和用户组。对于每一种版本的 UNIX，账户的管理会有一些不同，但是基础是一致的。创建一个用户的时候，通常把这个用户归属于默认组。当然，也可以把这个用户加到附加组中。当用户请求访问文件时，需要对文件的权限进行检查来确定用户的 ID 和工作组 ID 是否允许访问。

15.6 操作系统日志功能

当文件发生改变的时候，除了创建和比较检验和的值，管理员还需要监视系统的使

用和资源的访问情况。这些是由系统日志来完成的。目前的操作系统记录了很多事件用于之后的检测。系统日志是侦查和判断可疑行为的主要数据来源。但值得注意的是，尽管日志提供了丰富的信息，同样也需要大量的系统资源，需要耗费大量 CPU 时间来记录这些日志，需要更多的磁盘空间来存储日志文件。还需要一定的人力物力来管理和检查所有这些日志文件。

一个行之有效的日志记录方式是根据安全策略记录记录相应的安全事件。系统事件分为很多类。用户可以记录登录尝试、授权变更、资源访问、打印工作、性能指标等事件。可以使用这些日志来检查系统问题和可疑行为。日志提供的信息能够使用户追踪到某些人对系统做过的具体行为。

和其他的安全手段一样，设置合适的日志需要对自己的操作系统有着很好的了解。当系统具有更高的安全需求时，它应该记录更多的安全事件。一个存在更多风险的系统应该记录更多的事件。日志记录需求和系统功能之间的平衡决定着哪些事件需要被记录。

习　　题

一、选择题

1．注册表中，阻止访问特定驱动器内容的键值是下列哪一项？（　　）

A．NoViewOnDrive

B．RestrictRun

C．DisableRegistryTools

D．NoClose

2．以下 Windows 用户系统常见服务中，哪项是不能关闭的？（　　）

A．Internet 信息服务

B．远程登录

C．远程注册

D．注册表访问

二、问答题

1．简述安全操作系统必要的组成部分。

2．简述安全检查列表的重要性。

3．思考如何实现基本的文件系统安全。

课后实践与思考

Windows 主机操作系统加固规范实例

一、账号管理、认证授权

1．账号

SHG-Windows-01-01-01

编号	SHG-Windows-01-01-01
名称	按照用户类型分配账号
实施目的	根据系统的要求，设定不同的账户和账户组、管理员用户、数据库用户、审计用户、来宾用户等
问题影响	账号混淆，权限不明确，存在用户越权使用的可能
系统当前状态	进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”中记录当前用户状态

续表

编号	SHG-Windows-01-01-01
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”中结合要求和实际业务情况判断符合要求，根据系统的要求，设定不同的账户和账户组、管理员用户、数据库用户、审计用户、来宾用户
回退方案	删除新增加的用户，还原用户权限到初始设置。部分操作可能无法回退
判断依据	进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具->本地用户和组”中查看账户和账户组、管理员用户、数据库用户、审计用户、来宾用户等。根据系统的要求和实际业务情况判断是否符合要求
实施风险	高
重要等级	★★★
备注	

SHG-Windows-01-01-02

编号	SHG-Windows-01-01-02
名称	系统无效账户清理
实施目的	删除或锁定与设备运行、维护等与工作无关的账号，提高系统账户安全
问题影响	如果不清理无效账户，则系统将面临默认账号被非法利用的风险
系统当前状态	进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”中记录当前用户状态，备份系统 SAM 文件
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”中删除或锁定与设备运行、维护等与工作无关的账号
回退方案	增加被删除的用户，激活被锁定的用户，还原用户权限到初始设置。部分操作可能无法回退
判断依据	进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”中查看是否删除或锁定与设备运行、维护等与工作无关的账号 根据系统的要求和实际业务情况判断是否符合要求
实施风险	高
重要等级	★★★
备注	

SHG-Windows-01-01-03

编号	SHG-Windows-01-01-03
名称	重命名 Administrator，禁用 Guest
实施目的	对于管理员账号，要求更改默认账户名称；禁用 Guest（来宾）账号。提高系统安全性
问题影响	管理员账号容易被猜解；Guest 账号容易被非法利用
系统当前状态	进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”中记录当前用户状态
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”中执行以下操作。 Administrator→属性→更改名称 Guest 账号→属性→已停用

续表

编号	SHG-Windows-01-01-03
回退方案	重命名用户名称，还原用户属性设置
判断依据	进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”中 查看管理员账号 Administrator 名称是否修改，Guest 账号是否禁用。
实施风险	低
重要等级	★
备注	

2．口令

SHG-Windows-01-02-01

编号	SHG-Windows-01-02-01
名称	配置密码策略
实施目的	设置密码策略，减少密码安全风险；防止系统弱口令的存在，减少安全隐患。对于采用静态口令认证技术的设备，口令长度至少 6 位，且密码规则至少应采用字母（大小写穿插）加数字加标点符号（包括通配符）的方式
问题影响	增加系统密码被暴力破解的成功率
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“密码策略”：记录当前密码策略情况
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“密码策略”中，“密码必须符合复杂性要求”选择“已启动”，设置如下策略。
回退方案	还原密码策略到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“密码策略”中查看“密码必须符合复杂性要求”是否选择“已启动”
实施风险	低
重要等级	★★★
备注	

（实施步骤中的策略表）

策略	默认设置	推荐最低设置
强制执行密码历史记录	记住 1 个密码	记住 5 个密码
密码最长期限	42 天	90 天
密码最短期限	0 天	2 天
最短密码长度	0 个字符	8 个字符
密码必须符合复杂性要求	禁用	启用
为域中所有用户使用可还原的加密来储存密码	禁用	禁用

SHG-Windows-01-02-02

编号	SHG-Windows-01-02-02
名称	配置账户锁定策略
实施目的	设置有效的账户锁定策略有助于防止攻击者猜出系统账户的密码
问题影响	增加系统密码被暴力破解的成功率
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“账户锁定策略”中记录当前账户锁定策略情况
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“账户锁定策略”中设置如下策略 策略 / 默认设置 / 推荐最低设置 账户锁定时间 / 未定义 / 30 分钟 账户锁定阈值 / 0 / 6 次无效登录 复位账户锁定计数器 / 未定义 / 30 分钟
回退方案	还原账户锁定策略到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“账户锁定策略”中查看安全策略是否设置为已启动和按要求配置
实施风险	低
重要等级	★★★
备注	

（3）授权

SHG-Windows-01-03-01

编号	SHG-Windows-01-03-01
名称	远端系统强制关机设置
实施目的	防止远程用户非法关机，在本地安全设置中从远端系统强制关机只指派给 Administrators 组
问题影响	增加系统被管理员以外的用户非法关闭的风险
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看并记录“从远端系统强制关机”的当前设置
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中将“从远端系统强制关机”设置为“只指派给 Administrators 组”
回退方案	还原“从远端系统强制关机”的设置到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看“从远端系统强制关机”是否设置为“只指派给 Administrators 组”
实施风险	低
重要等级	★★★
备注	

SHG-Windows-01-03-02

编号	SHG-Windows-01-03-02
名称	关闭系统设置
实施目的	防止管理员以外的用户非法关机，在本地安全设置中关闭系统仅指派给 Administrators 组
问题影响	增加系统被管理员以外的用户非法关闭的风险
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看并记录“关闭系统”的当前设置
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中将“关闭系统”设置为“只指派给 Administrators 组”
回退方案	还原“关闭系统”的设置到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看“关闭系统”是否设置为“只指派给 Administrators 组”
实施风险	低
重要等级	★★★
备注	

SHG-Windows-01-03-03

编号	SHG-Windows-01-03-03
名称	“取得文件或其他对象的所有权”设置
实施目的	防止用户非法获取文件，在本地安全设置中取得文件或其他对象的所有权仅指派给 Administrators
问题影响	增加系统除管理员以外的用户非法获取文件的风险
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看并记录“取得文件或其他对象的所有权”的当前设置
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中将“取得文件或其他对象的所有权”设置为“只指派给 Administrators 组”
回退方案	还原“取得文件或其他对象的所有权”的设置到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看是否“取得文件或其他对象的所有权”设置为“只指派给 Administrators 组”
实施风险	低
重要等级	★★★
备注	

SHG-Windows-01-03-04

编号	SHG-Windows-01-03-04
名称	“从本地登录此计算机”设置
实施目的	防止用户非法登录主机，在本地安全设置中配置指定授权用户允许本地登录此计算机

续表

编号	SHG-Windows-01-03-04
问题影响	增加物理临近攻击和本地物理攻击以及非授权用户非法登录主机的风险
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看并记录“从本地登录此计算机”的当前设置
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中将“从本地登陆此计算机”设置为“指定授权用户”
回退方案	还原“从本地登录此计算机”的设置到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看是否“从本地登录此计算机”设置为“指定授权用户”
实施风险	低
重要等级	★★★
备注	

SHG-Windows-01-03-05

编号	SHG-Windows-01-03-05
名称	“从网络访问此计算机”设置
实施目的	防止网络用户非法访问主机，在组策略中只允许授权账号从网络访问（包括网络共享等，但不包括终端服务）此计算机
问题影响	增加非授权用户非法访问主机的风险
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看并记录“从网络访问此计算机”的当前设置
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中将“从网络访问此计算机”设置为“指定授权用户”
回退方案	还原“从网络访问此计算机”的设置到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”中查看是否“从网络访问此计算机”设置为“指定授权用户”
实施风险	低
重要等级	★★★
备注	

二、日志配置

SHG-Windows-02-01-01

编号	SHG-Windows-02-01-01
名称	审核策略设置
实施目的	设置审核策略，记录系统重要的事件日志，设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址
问题影响	无法对用户的登录以及登录后对系统的操作过程、特权使用等进行日志记录
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，查看并记录“审核策略”的当前设置

续表

编号	SHG-Windows-02-01-01
实施步骤	参考配置操作： “开始”→“运行”→“执行“控制面板”→“管理工具”→“本地安全策略”→“审核策略” 审核登录事件，双击，设置为成功和失败都审核。 “审核策略更改”设置为“成功”和“失败”都要审核 “审核对象访问”设置为“成功”和“失败”都要审核 “审核目录服务器访问”设置为“成功”和“失败”都要审核 “审核特权使用”设置为“成功”和“失败”都要审核 “审核系统事件”设置为“成功”和“失败”都要审核 “审核账户管理”设置为“成功”和“失败”都要审核 “审核过程追踪”设置为“失败”需要审核
回退方案	还原“审核策略”的设置到加固之前配置
判断依据	“开始”→“运行”→“执行”“控制面板”→“管理工具”→“本地安全策略”→“审核策略”： 查看是否设置为成功和失败都审核
实施风险	低
重要等级	★★★
备注	

SHG-Windows-02-01-02

编号	SHG-Windows-02-01-02
名称	日志记录策略设置
实施目的	优化系统日志记录，防止日志溢出。设置应用日志文件大小至少为 8192KB，设置当达到最大的日志尺寸时，按需要改写事件
问题影响	如果日志的大小超过系统默认设置，则无法正常记录超过最大记录值后的所有系统日志、应用日志、安全日志等
系统当前状态	进入“控制面板”→“管理工具”→“事件查看器”，查看并记录“应用日志”、“系统日志”、“安全日志”的当前设置
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“事件查看器”，在“事件查看器（本地）”中： “应用日志”属性中的日志大小设置不小于“8192KB”，设置当达到最大的日志尺寸时，“按需要改写事件” “系统日志”属性中的日志大小设置不小于“8192KB”，设置当达到最大的日志尺寸时，“按需要改写事件” “安全日志”属性中的日志大小设置不小于“8192KB”，设置当达到最大的日志尺寸时，“按需要改写事件”
回退方案	还原“应用日志”、“系统日志”、“安全日志”的设置到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“事件查看器”，在“事件查看器（本地）”中： 查看各项日志属性中日志大小是否设置为不小于“8192KB”，是否设置当达到最大的日志尺寸时，“按需要改写事件”
实施风险	低
重要等级	★
备注	

三、通信协议

IP 协议安全

SHG-Windows-03-01-01

编号	SHG-Windows-03-01-01
名称	启用 TCP/IP 筛选
实施目的	过滤不必要的端口，提高系统安全性，对没有自带防火墙的 Windows 系统，启用 Windows 系统的 IP 安全机制（IPSec）或网络连接上的 TCP/IP 筛选，只开放业务所需要的 TCP、UDP 端口和 IP 协议
问题影响	如不有效过滤系统中存在的不必要的端口以及默认的端口会增加潜在被攻击和非法利用的安全风险
系统当前状态	进入“控制面板”→“网络连接”→“本地连接”，进入“Internet 协议（TCP/IP）属性”→“高级 TCP/IP 设置”，在“选项”的属性中查看“网络连接上的 TCP/IP 筛选”的状态，并记录
实施步骤	参考配置操作： 系统管理员出示业务所需端口列表。 根据列表只开放系统与业务所需端口。 进入“控制面板”→“网络连接”→“本地连接”，进入“Internet 协议（TCP/IP）属性”→“高级 TCP/IP 设置”，在“选项”的属性中启用网络连接上的 TCP/IP 筛选，只开放业务所需要的 TCP、UDP 端口和 IP 协议
回退方案	还原高级 TCP/IP 的设置到加固之前配置
判断依据	系统管理员出示业务所需端口列表。 根据列表只开放系统与业务所需端口。 进入“控制面板”→“网络连接”→“本地连接”，进入“Internet 协议（TCP/IP）属性”→“高级 TCP/IP 设置”，在“选项”的属性中启用网络连接上的 TCP/IP 筛选，查看是否只开放业务所需要的 TCP、UDP 端口和 IP 协议。 利用 Netstat–an 命令查看当前系统开放端口是否与系统管理员所出示的业务所需端口列表相对应；如发现存在与业务和应用无关的端口，则查明后在 TPC/IP 筛选配置中将其过滤掉
实施风险	高
重要等级	★
备注	

SHG-Windows-03-01-02

编号	SHG-Windows-03-01-01
名称	开启系统防火墙
实施目的	启用 Windows XP 和 Windows 2003 自带防火墙，过滤不必要的端口，提高系统安全性。根据业务需要限定允许访问网络的应用程序和允许远程登陆该设备的 IP 地址范围
问题影响	没有访问控制，系统可能被非法登录或使用，从而增加潜在被攻击的安全风险
系统当前状态	进入“控制面板”→“网络连接”→“本地连接”，在高级选项的属性中查看 Windows 防火墙的状态，并记录详细情况

续表

编号	SHG-Windows-03-01-01
实施步骤	参考配置操作： 系统管理员出示业务所需端口列表。 根据列表只开放系统与业务所需端口。 进入“控制面板”→“网络连接”→“本地连接”，在高级选项的设置中启用 Windows 防火墙。 在“例外”中配置允许业务所需的程序接入网络。 在“例外”→“编辑”→“更改范围”中编辑允许接入的网络地址范围
回退方案	还原高级系统防火墙设置到加固之前配置。
判断依据	进入“控制面板”→“网络连接”→“本地连接”，在高级选项的设置中，查看是否启用 Windows 防火墙。 查看是否在“例外”中配置允许业务所需的程序接入网络。 查看是否在“例外”→“编辑”→“更改范围”中编辑允许接入的网络地址范围
实施风险	高
重要等级	★
备注	

SHG-Windows-03-01-03

编号	SHG-Windows-03-01-03
名称	启用 SYN 攻击保护
实施目的	启用 SYN 攻击保护，提高系统安全性；指定触发 SYN 洪水攻击保护所必须超过的 TCP 连接请求数阀值为 5；指定处于 SYN_RCVD 状态的 TCP 连接数的阈值为 500；指定处于至少已发送一次重传的 SYN_RCVD 状态中的 TCP 连接数的阈值为 400
问题影响	如不启用 SYN 攻击保护，系统则容易被 SYN 拒绝服务攻击后导致迅速宕机
系统当前状态	在“开始”→“运行”中输入 regedit 查看并记录注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services、SynAttackProtect 的值并记录。 查看并记录注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 之下 TcpMaxPortsExhausted TcpMaxHalfOpen TcpMaxHalfOpenRetried 的值并记录
实施步骤	参考配置操作： 在“开始”→“运行”中输入 regedit 启用 SYN 攻击保护的命名值位于注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 之下。值名称：SynAttackProtect。推荐值：2。 以下部分中的所有项和值均位于注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 之下。 指定必须在触发 SYN flood 保护之前超过的 TCP 连接请求阈值。值名称：TcpMaxPortsExhausted。推荐值：5。

续表

编号	SHG-Windows-03-01-03
实施步骤	启用 SynAttackProtect 后，该值指定 SYN_RCVD 状态中的 TCP 连接阈值，超过 SynAttackProtect 时，触发 SYN flood 保护。值名称：TcpMaxHalfOpen。推荐值数据：500。 启用 SynAttackProtect 后，指定至少发送了一次重传的 SYN_RCVD 状态中的 TCP 连接阈值。超过 SynAttackProtect 时，触发 SYN flood 保护。值名称：TcpMaxHalfOpenRetried。推荐值数据：400。
回退方案	还原注册表设置到加固之前配置
判断依据	在“开始”→“运行”中输入 regedit，进入注册表中打开相应的注册项，查看键值是否已启用和配置，各注册表键值是否均按要求设置
实施风险	高
重要等级	★
备注	

四、设备其他安全要求

1．屏幕保护

SHG-Windows-04-01-01

编号	SHG-Windows-04-01-01
名称	启用屏幕保护程序
实施目的	启用屏幕保护程序，防止管理员忘记锁定机器被非法攻击；设置带密码的屏幕保护，并将时间设定为 5 分钟
问题影响	如未启动屏幕保护并采用密码恢复，一旦管理员操作系统后忘记锁定主机，则容易被非法攻击，以及增加本地物理临近攻击的风险
系统当前状态	进入“控制面板”→“显示”→“屏幕保护程序”： 查看是否启用屏幕保护程序并记录当前的设置
实施步骤	参考配置操作： 进入“控制面板”→“显示”→“屏幕保护程序”： 启用屏幕保护程序，设置等待时间为“5 分钟”，启用“在恢复时使用密码保护”
回退方案	还原屏幕保护程序设置到加固之前配置
判断依据	进入“控制面板”→“显示”→“屏幕保护程序”： 查看是否启用屏幕保护程序，设置等待时间为“5 分钟”，启用“在恢复时使用密码保护” 在系统桌面上右击，打开属性，查看屏幕保护程序选项是否已启动和配置
实施风险	低
重要等级	★★★
备注	

SHG-Windows-04-01-02

编号	SHG-Windows-04-01-02
名称	设置 Microsoft 网络服务器挂起时间
实施目的	设置 Microsoft 网络服务器挂起时间，防止管理员忘记锁定机器被非法利用；对于远程登录的账号，设置不活动断连时间 15 分钟
问题影响	管理员忘记锁定而被非法利用
系统当前状态	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略->安全选项”中查看是否“Microsoft 网络服务器”设置为“在挂起会话之前所需的空闲时间”为 15 分钟
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“安全选项”中将“Microsoft 网络服务器”设置为“在挂起会话之前所需的空闲时间”为 15 分钟
回退方案	还原“挂起会话之前所需的空闲时间”设置到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“安全选项”中查看是否“Microsoft 网络服务器”设置为“在挂起会话之前所需的空闲时间”为 15 分钟
实施风险	低
重要等级	★★★
备注	

2．共享文件夹及访问权限

SHG-Windows-04-02-01

编号	**SHG-Windows-04-02-01**
名称	关闭默认共享
实施目的	非域环境中，关闭 Windows 硬盘默认共享，例如 C$、D$，提高系统安全性能
问题影响	防止攻击者利用系统默认共享如 C$、D$等，非法对系统的硬盘进行访问，以及通过 IPC$方式暴力破解账户和密码
系统当前状态	查看并记录注册表 HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\增加了 REG_DWORD 类型的 AutoShareServer 键的值
实施步骤	参考配置操作： 进入“开始”→“运行”→Regedit，进入注册表编辑器， 更改注册表键值：在 HKLM\System\CurrentControlSet\ Services\LanmanServer\Parameters\下，增加 REG_DWORD 类型的 AutoShareServer 键，值为 0
回退方案	还原“AutoShareServer”键的值设置到加固之前配置
判断依据	进入“开始”→“运行”→“Regedit”，进入注册表编辑器，查看 HKLM\System\CurrentControlSet\ Services\LanmanServer\Parameters\下，是否已增加 REG_DWORD 类型的 AutoShareServer 键，值为 0
实施风险	低
重要等级	★
备注	

SHG-Windows-04-02-02

编号	SHG-Windows-04-02-02
名称	设置共享文件夹访问权限
实施目的	设置共享文件夹访问权限，防止用户非法访问。只允许授权的账户拥有权限共享此文件夹
问题影响	增加系统未授权的用户非法访问共享文件夹的风险
系统当前状态	进入“控制面板”→“管理工具”→“计算机管理”，进入“系统工具”→“共享文件夹”：查看并记录每个共享文件夹的共享权限
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“计算机管理”，进入“系统工具”→“共享文件夹”：查看每个共享文件夹的共享权限，只将权限授权于指定账户
回退方案	还原每个共享文件夹的共享权限到加固之前配置
判断依据	进入“控制面板”→“管理工具”→“计算机管理”，进入“系统工具”→“共享文件夹”：查看每个共享文件夹的共享权限 查看每个共享文件夹的共享权限是否仅限于业务需要，不设置成为“everyone”
实施风险	低
重要等级	★★★
备注	

3．补丁管理

SHG-Windows-04-03-01

编号	SHG-Windows-04-03-01
名称	安装系统补丁
实施目的	修复系统漏洞。应安装最新的 Service Pack 补丁集。对服务器系统应先进行兼容性测试
问题影响	如系统未打补丁或补丁未打全，不是最新的补丁，则面临容易被攻击、渗透和控制的风险
系统当前状态	进入“控制面板”→“添加或删除程序”，选中“显示更新”复选框，查看并记录当前系统安装的补丁
实施步骤	参考配置操作： 安装最新的 Service Pack 补丁集，以及最新的 Hotfix 补丁。目前 Windows XP 的 Service Pack 为 SP3 Windows2000 的 Service Pack 为 SP4，Windows 2003 的 Service Pack 为 SP2
回退方案	卸载新安装的补丁
判断依据	进入“控制面板”→“添加或删除程序”，选中“显示更新”复选框，查看是否 XP 系统已安装 SP3，Win2000 系统已安装 SP4，Win2003 系统已安装 SP2。同时检查所有的 hotfix，并查看系统安装的最后一个补丁的发布日期是否与最近最新发布的补丁日期一致
实施风险	高
重要等级	★★★
备注	

4．防病毒管理

SHG-Windows-04-04-01

编号	SHG-Windows-04-04-01
名称	安装、更新杀毒软件
实施目的	安装防病毒软件，并及时更新，提高系统防病毒能力
问题影响	如系统中未安装防病毒软件或防病毒软件未及时更新，则系统面临容易被病毒感染的风险
系统当前状态	查看是否安装杀毒软件；打开防病毒软件控制面板，查看病毒码更新日期
实施步骤	参考配置操作： 安装防病毒软件，并将病毒库更新到最新的版本
回退方案	卸载或删除杀毒软件
判断依据	进入“控制面板”→“添加或删除程序”，查看是否安装有防病毒软件。同时打开防病毒软件控制面板，查看病毒码更新日期。 如已安装防病毒软件，则病毒码更新时间不早于 1 个月，各系统病毒码升级时间要求参见各系统相关规定
实施风险	低
重要等级	★★★
备注	

SHG-Windows-04-04-02

编号	SHG-Windows-04-04-02
名称	数据执行保护配置
实施目的	提高系统抵抗非法修改文件的性能。对于 Windows XP SP2 及 Windows 2003 对 Windows 操作系统程序和服务启用系统自带 DEP 功能（数据执行保护），防止在受保护内存位置运行有害代码
问题影响	如未配置系统核心的数据执行保护，则无法对在内存位置运行有害代码进行保护
系统当前状态	进入“控制面板”→“系统”，单击“高级”选项卡的“性能”下的“设置”按钮，进入“数据执行保护”选项卡，查看并记录“仅为基本 Windows 操作系统程序和服务启用 DEP”的配置状态
实施步骤	参考配置操作： 进入“控制面板”→“系统”，单击“高级”选项卡的“性能”下的“设置”按钮，进入“数据执行保护”选项卡，设置为“仅为基本 Windows 操作系统程序和服务启用 DEP”
回退方案	将“仅为基本 Windows 操作系统程序和服务启用 DEP”设置到加固前配置
判断依据	进入“控制面板”→“系统”，单击“高级”选项卡的“性能”下的“设置”按钮，进入“数据执行保护”选项卡，查看是否设置为“仅为基本 Windows 操作系统程序和服务启用 DEP”
实施风险	低
重要等级	★
备注	

5．Windows 服务

SHG-Windows-04-05-01

编号	SHG-Windows-04-05-01
名称	关闭服务
实施目的	关闭系统不必要的服务，提高系统安全性。列出所需要服务的列表（包括所需的系统服务），不在此列表的服务需关闭
问题影响	如不关闭与业务和应用无关或不必要的服务，则系统面临容易被攻击、渗透或利用的风险
系统当前状态	运行命令 net start 查看当前运行的服务
实施步骤	参考配置操作： 进入“控制面板”→“管理工具”→“计算机管理”，进入“服务和应用程序”：查看所有服务，不在此列表的服务需关闭

服务	启动类型	包括在成员服务器基准策略中的理由
COM+事件服务	手动	允许组件服务的管理
DHCP 客户端	自动	更新动态 DNS 中的记录所需
分布式链接跟踪客户端	自动	用来维护 NTFS 卷上的链接
DNS 客户端	自动	允许解析 DNS 名称
事件日志	自动	允许在事件日志中查看事件日志消息
逻辑磁盘管理器	自动	需要它来确保动态磁盘信息保持最新
逻辑磁盘管理器管理服务	手动	需要它以执行磁盘管理
Netlogon	自动	加入域时所需
网络连接	手动	网络通信所需
性能日志和警报	手动	收集计算机的性能数据，向日志中写入或触发警报
即插即用	自动	Windows 标识和使用系统硬件时所需
受保护的存储区	自动	需要用它保护敏感数据，如私钥
远程过程调用（RPC）	自动	Windows 中的内部过程所需
远程注册服务	自动	hfnetchk 实用工具所需（参见附注）
安全账户管理器	自动	存储本地安全账户的账户信息
服务器	自动	hfnetchk 实用工具所需（参见附注）
系统事件通知	自动	在事件日志中记录条目所需
TCP/IP NetBIOS Helper 服务	自动	在组策略中进行软件分发所需（可用来分发修补程序）
Windows 管理规范驱动程序	手动	使用“性能日志和警报”实现性能警报时所需
Windows 时间服务	自动	需要它来保证 Kerberos 身份验证有一致的功能
工作站	自动	加入域时所需

续表

编号	SHG-Windows-04-05-01
回退方案	进入“控制面板”→“管理工具”→“计算机管理”，进入“服务和应用程序”，配置并启动停止的服务
判断依据	系统管理员应出具系统所必要的服务列表。 查看所有服务，不在此列表的服务需关闭。 进入“控制面板”→“管理工具”→“计算机管理”，进入“服务和应用程序”：查看所有服务，不在此列表的服务是否已关闭
实施风险	中
重要等级	★★★
备注	

SHG-Windows-04-05-02

编号	SHG-Windows-04-05-02
名称	修改 SNMP 服务密码
实施目的	修改 SNMP 服务密码，防止泄露系统信息。如需启用 SNMP 服务，则修改默认的 SNMP Community String 设置
问题影响	如未修改 SNMP 服务的默认密码，则攻击者利用 SNMP 信息探测工具就可以获取系统信息。从而增加系统被攻击的风险
系统当前状态	打开“控制面板”，打开“管理工具”中的“服务”，找到“SNMP Service”，右击打开“属性”面板中的“安全”选项卡，查看 community strings 的值
实施步骤	参考配置操作： 打开“控制面板”，打开“管理工具”中的“服务”，找到“SNMP Service”，右击打开“属性”面板中的“安全”选项卡，在这个配置界面中，可以修改 community strings，也就是微软所说的“团体名称”
回退方案	修改 community strings 值到加固前状态
判断依据	打开“控制面板”，打开“管理工具”中的“服务”，找到“SNMP Service”，右击打开“属性”面板中的“安全”选项卡，在这个配置界面中，查看 community strings 是否已改，而不是默认的“public”
实施风险	中
重要等级	★
备注	

6．启动项

SHG-Windows-04-06-01

编号	SHG-Windows-04-06-01
名称	关闭无效启动项
实施目的	关闭无效的服务，提高系统性能，增加系统安全性。列出系统启动时自动加载的进程和服务列表，不在此列表的需关闭
问题影响	如不禁用和关闭与业务和应用无关或不必要的启动项和进程，则系统面临容易被攻击、渗透或利用的风险
系统当前状态	查看记录在“开始”→“运行”中输入 MSconfig，启动菜单中各项配置参数
实施步骤	参考配置操作： 在“开始”→“运行”中输入 MSconfig，取消不必要的启动项

续表

编号	SHG-Windows-04-06-01
回退方案	在“开始”→“运行”中输入 MSconfig，还原各项启动参数到加固前状态
判断依据	系统管理员提供业务必须的自动加载进程和服务列表文档。 在“开始”→“运行”中输入 MSconfig： 不需要的自动加载进程是否已禁用和取消
实施风险	中
重要等级	★★★
备注	

SHG-Windows-04-06-02

编号	SHG-Windows-04-06-02
名称	关闭 Windows 自动播放功能
实施目的	关闭 Windows 自动播放，防止从移动设备感染病毒
问题影响	如不关闭 Windows 自动播放，则在进行 U 盘插入操作的时候，系统将面临被 U 盘中的病毒感染的风险
系统当前状态	单击“开始”→“运行”命令，输入 gpedit.msc，打开组策略编辑器，浏览到“计算机配置”→“管理模板”→“系统”，查看各驱动器“关闭自动播放”状态
实施步骤	参考配置操作： 单击“开始”→“运行”命令，输入 gpedit.msc，打开组策略编辑器，浏览到“计算机配置”→“管理模板”→“系统”，在右边窗格中双击“关闭自动播放”，对话框中选择所有驱动器，确定即可
回退方案	打开组策略编辑器，浏览到“计算机配置”→“管理模板”→“系统”，还原驱动器“关闭自动播放”状态
判断依据	单击“开始”→“运行”命令，输入 gpedit.msc，打开组策略编辑器，浏览到“计算机配置”→“管理模板”→“系统”： 查看是否所有驱动器均选择“关闭自动播放”，查看“关闭自动播放”配置是否已启用，启用范围：所有驱动器
实施风险	低
重要等级	★★★
备注	

第 16 章　安全审计原则与实践

本章学习重点：

- 在不同的环境中记录合适的系统事件
- 识别安全事件并迅速通报安全管理员
- 解释 Window 与 UNIX 的系统日志
- 判断入侵事件的发生
- 使用通用的审计工具和技术管理系统安全审计

日志记录与审计是系统信息安全中最为繁琐的两个环节，这些工作单调并且耗时。但这些工作同样也是安全实践中最为重要的众多工作。本章会介绍如何恰当地进行这些工作，并以此加强组织的安全环境。

16.1　设置日志记录

当启动一个日志记录程序时，首先要对该程序的初始值进行一系列的设置，以下几个因素是需要考虑的重点。

（1）需要记录的行为内容。

（2）日志记录需要保存的时间。

（3）何种事件发生后，应在第一时间对安全管理员进行报警？

16.1.1　需要记录的行为

目前很多安全管理员的想法是记录系统中的每一个事件。这种方案可以避免安全事件的遗漏，但缺点是日志记录程序的效率太低，原因如下。

（1）该方案会制造出大量的日志文件，导致繁重的审阅工作。

（2）过度的记录日志会导致系统性能下降。记录日志会消耗一定的系统资源，在普通环境下影响不大，但在记录日志过多的情况下，系统的资源就大量消耗，导致性能大幅下降。

（3）一些关键事件可能被覆盖。很多组织将日志文件存储在特定的地方，如果该位置的存储能力有限，在日志文件大小超出其存储空间时，有些日志文件就可能被覆盖，从而导致一些真正危害系统的事件不能被发现。

因此就需要明确应该对系统的哪些事件做出记录。下面通过一个例子说明要根据具体的环境来确定日志记录的内容。

有张三和李四两个安全管理员，张三是一个政府机构的管理员，而李四是一家新闻网站部门的管理员，两个人的工作都是负责保护组织系统的安全。但两个人工作的侧重点是不同的，张三在保证其网络安全时，更关注信息安全的保密性（如果发生信息泄露，

会对社会安全造成破坏）、完整性（政府信息常用于决策制定等关系重大的事件，必须保证其准确性）和可用性（政府决策人员必须不断通过信息来进行相关决策）。因此要求其日志记录能够在任意一个属性受到损坏后能及时对管理员进行通报。

李四却有着不同的安全需求。作为一个公共的新闻平台，网站上所有的信息对公众都是开放的，因此不需要考虑保密性。然而，信息的完整性和可用性则是需要考虑的，如果完整性受损，那么公众接受的信息就有可能不真实，从而降低公信力；如果可用性降低，用户就无法在网站上获取信息，会转投到其他的竞争网站上获取信息。因此，李四不需要记录文件存取这样的事件（这样会产生大量的无用记录），但需要建立防止网站非授权修改和拒绝服务攻击尝试的日志程序。

16.1.2 记录保留时间

每个操作系统都允许对日志记录进行自动存储，但会根据时间或存储空间的规则覆盖相应的日志文件，具体使用哪种规则需要安全管理人员根据安全的优先级来判断。如果关注存储日志记录时的系统资源消耗，就应当在记录大小达到特定的参数后对原来的记录进行覆盖，以防止其占用额外的硬盘资源。如果关注的是一个特定时间段的日志记录，就应该使用基于时间的覆盖原则，对旧的日志文件进行删除操作前对其进行备份。最好是建立两个独立的日志文件，一个文件记录完毕后，转向下一个文件进行记录，同时将已经记录完毕的文件及时进行备份，从而进行循环，这样就可以对一段时间的系统行为进行记录。

16.1.3 设置报警系统

目前，主流的操作系统都可以在特定安全事件发生后对安全管理员进行报警，这样可以在安全事件发生的第一时间就使得安全管理员了解到事件的情况，并采取及时有效的措施。

系统报警形式主要包括电子邮件、纸质报告、短信、即时通信、电话等多种形式。报警机制可由以上多种方式组成。

16.1.4 Windows 日志记录

Windows 操作系统中优先级最高的记录机制是事件查看器，其允许系统记录不同类型的系统事件。所有的 Windows 系统都有 3 种基本的日志文件。

- **安全日志**　该日志包括发生在系统中与安全相关的事件，具体需要记录的内容由系统管理员控制。几个典型的安全日志记录包括尝试登录失败、尝试越权以及类似的系统事件。
- **应用日志**　该日志记录的是系统中启动应用程序的事件，由每个软件包决定该日志的内容。除了记录程序的名字以外，该日志同样记录与某些应用程序相关的核心安全信息。例如，应用日志会记录未能成功删除数据库中某数据的行为。

- **系统日志** 该日志记录的是与操作系统有关的事件。例如软件/硬件故障和其他的系统问题，具体的内容是由操作系统预设的。图 16-1 简单列举了某个系统查看器的系统日志的部分信息。

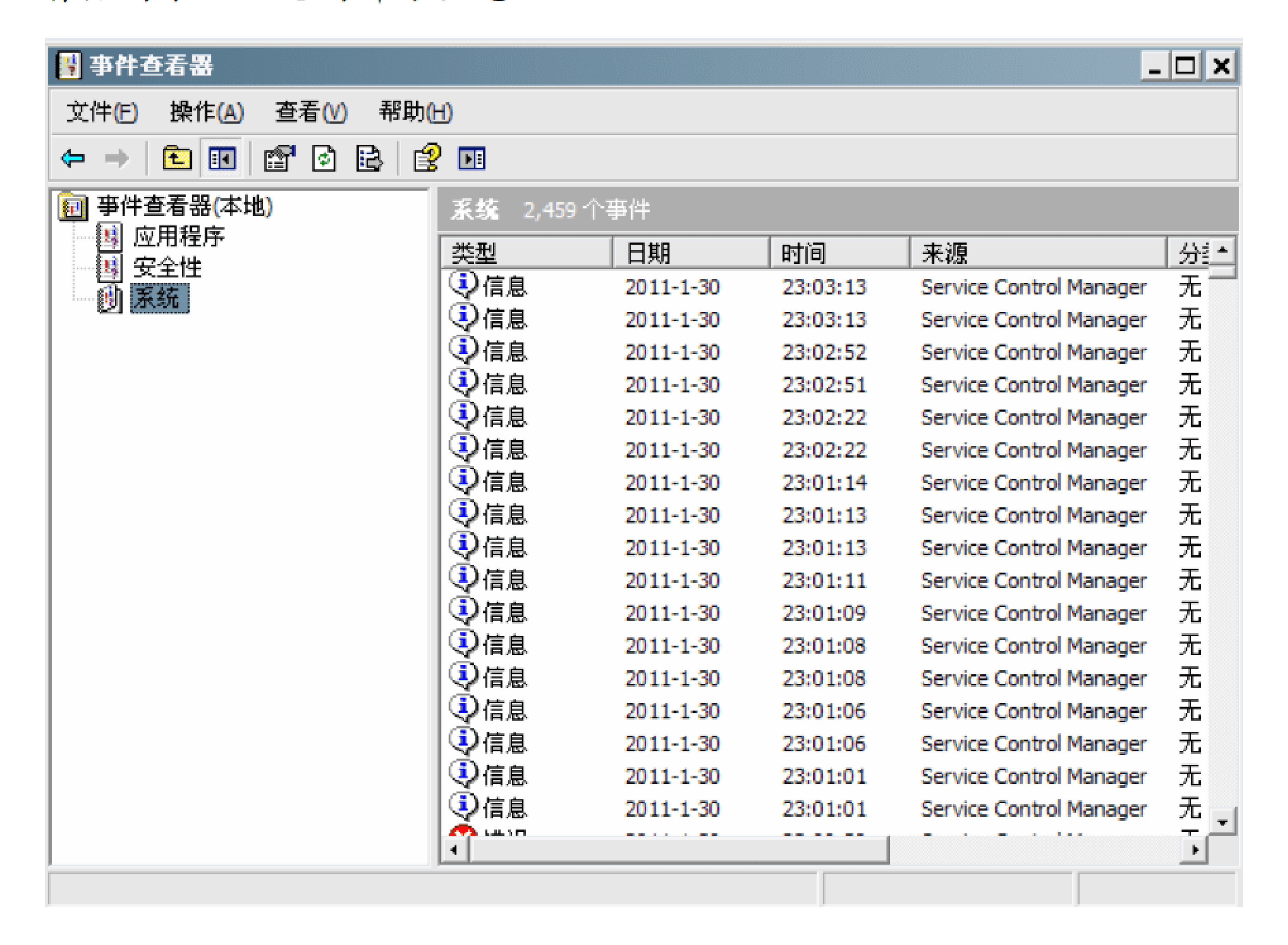


图 16-1　事件查看器

除以上 3 种基本的日志类型外，还有以下几种日志记录。

- **目录服务日志** 该日志存储在 Windows 域控制器中，主要内容是与 Windows 目录服务有关的事件记录。
- **文件复制服务日志** 该日志存储在域控制器中，主要内容是通过文件复制服务复制数据的事件的记录。
- **错误日志** 该日志记录的事件为系统内发生重大故障的事件。
- **警告日志** 该日志向系统管理员报告系统内存在的潜在安全问题，例如当一个硬盘存放的数据达到其承受的最大值时，会及时触发安全警报。
- **信息日志** 记录内容有系统管理员设定，一般是系统运行情况，但并不会反映系统安全隐患的内容。例如，信息日志中可能记录系统正常启动或正常停止某一进程这一事件。

16.1.5 UNIX 日志记录

UNIX 系统通过使用 syslog 日志函数来记录日志，同样在 UNIX 类操作系统上，syslog 广泛应用于系统日志。syslog 日志消息既可以记录在本地文件中，也可以通过网络发送到接收 syslog 的服务器。接收 syslog 的服务器可以对多个设备的 syslog 消息进行统一的存储，或解析其中的内容做相应的处理。常见的应用场景是网络管理工具、安全管理系

统、日志审计系统。完整的 syslog 日志包含产生日志的程序模块、时间、主机名或 IP 地址、进程名、进程 ID 和正文等消息，如图 16-2 所示。在 UNIX 类操作系统上，能够按相关信息决定需要记录哪些日志消息，记录到什么地方，是否需要发送到一个 syslog 接收服务器等。

```
Aug 18 12:33:00 bt kernel: imklog 4.2.0, log source = /proc/kmsg started.
Aug 18 12:33:00 bt rsyslogd: [origin software="rsyslogd" swVersion="4.2.0" x-pid="427" x-info="http://www.r
syslog.com"] (re)start
Aug 18 12:33:00 bt rsyslogd: rsyslogd's groupid changed to 103
Aug 18 12:33:00 bt rsyslogd: rsyslogd's userid changed to 101
Aug 18 12:33:00 bt rsyslogd-2039: Could no open output file '/dev/xconsole' [try http://www.rsyslog.com/e/2
039 ]
Aug 18 12:33:00 bt kernel: [    0.000000] Initializing cgroup subsys cpuset
Aug 18 12:33:00 bt kernel: [    0.000000] Initializing cgroup subsys cpu
Aug 18 12:33:00 bt kernel: [    0.000000] Linux version 2.6.39.4 (root@builder32) (gcc version 4.4.3 (Ubunt
u 4.4.3-4ubuntu5) ) #1 SMP Thu Aug 18 13:38:02 NZST 2011
Aug 18 12:33:00 bt kernel: [    0.000000] KERNEL supported cpus:
Aug 18 12:33:00 bt kernel: [    0.000000]   Intel GenuineIntel
Aug 18 12:33:00 bt kernel: [    0.000000]   AMD AuthenticAMD
Aug 18 12:33:00 bt kernel: [    0.000000]   NSC Geode by NSC
Aug 18 12:33:00 bt kernel: [    0.000000]   Cyrix CyrixInstead
Aug 18 12:33:00 bt kernel: [    0.000000]   Centaur CentaurHauls
Aug 18 12:33:00 bt kernel: [    0.000000]   Transmeta GenuineTMx86
Aug 18 12:33:00 bt kernel: [    0.000000]   Transmeta TransmetaCPU
Aug 18 12:33:00 bt kernel: [    0.000000]   UMC UMC UMC UMC
Aug 18 12:33:00 bt kernel: [    0.000000] BIOS-provided physical RAM map:
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 0000000000000000 - 000000000009f800 (usable)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 000000000009f800 - 00000000000a0000 (reserved)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 00000000000ca000 - 00000000000cc000 (reserved)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 00000000000dc000 - 00000000000e4000 (reserved)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 00000000000e8000 - 0000000000100000 (reserved)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 0000000000100000 - 000000002fef0000 (usable)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 000000002fef0000 - 000000002feff000 (ACPI data)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 000000002feff000 - 000000002ff00000 (ACPI NVS)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 000000002ff00000 - 0000000030000000 (usable)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 00000000e0000000 - 00000000f0000000 (reserved)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 00000000fec00000 - 00000000fec10000 (reserved)
Aug 18 12:33:00 bt kernel: [    0.000000]  BIOS-e820: 00000000fee00000 - 00000000fee01000 (reserved)
--More--(0%)
```

图 16-2　syslog 部分内容

和 Windows 的事件查看器一样，syslog 也允许操作系统和其他的程序对每一个具体的事件制定具体的优先级，从而提供一个可变、灵活的日志记录报警机制。具体来说，有 8 种优先级别，级别由高到低依次如下。

- **LOG_EMERG**　表示该事件属于紧急事件，要求通知所有系统用户。
- **LOG_ALERT**　要求系统管理员立刻对系统进行备份，表示当前状态需要修正。
- **LOG_CRIT**　一般硬件错误。
- **LOG_ERR**　一般系统故障，严重性没有上一级高。
- **LOG_WARNING**　由系统管理员定义的一些事件，由系统不安全状态引起，用于了解系统的当前安全状态是否受损。
- **LOG_NOTICE**　同样是由系统管理员定义的一些事件，但并不包含所有的系统不安全状态。
- **LOG_INFO**　提供一些信息供日后使用。
- **LOG_DEBUG**　调试程序时的信息。

16.2　日志数据分析

对系统进行日志记录之后要通过分析这些数据对系统环境进行监控。具体有两个操

作：建立正常行为轮廓，监测异常的行为。

1．建立正常行为基准

分析日志文件的第一步就是先了解哪些行为属于正常行为，这些正常行为也可以称为行为基准。这些行为基准就是不同的系统在不同环境中、不同时间段中的正常系统资源消耗，将用于日后的异常行为监测。不同时间段或不同环境下的系统基准是不一样的。例如，某一商业系统在工作时段的基准与在周末时段的基准是不一样的。

作为系统管理员，要为系统确定合适的基准来监测系统的故障。在设置准确的基准后，还需要在日常的系统运行中对其进行监测，根据系统的变化对基准进行适当的修改。

2．监测异常行为

建立系统基准之后，下一步就是监测异常行为，需要考虑以下几方面因素。

（1）行为偏离系统基准的程度

首先要确定系统基准行为的阈值，不同系统的相应阈值是不同的。例如，统计两个系统的行为参数，两个系统 CPU 利用率的平均值都为 45%，其中一个系统的 CPU 利用率浮动在 10%～60%之间，另一个系统的 CPU 利用率浮动在 5%～90%之间。可以通过以上数据确定第一个系统 CPU 利用率的阀值为 65%，第二个系统 CPU 利用率的阀值为 95%。

（2）偏差行为发生的时间

某些正常情况下，系统的行为也有可能超出基准的阈值范围。确定这些行为是否为异常事件还要取决于行为持续的时间。根据不同的系统及不同的安全需求，时间标准是不同的。利用上面的例子，对于第一个系统，如果系统 CPU 利用率超过 65%的情况持续两分钟以上，则被认定为异常事件，而第二个系统 CPU 利用率超过 95%的情况持续半分钟就被认定为异常事件。

（3）需要报告的异常事件类型

每个系统都存在着一些更能说明系统正在遭受安全威胁的事件，这类事件就应立刻向系统管理员报告。如果硬盘中存放着企业信息的数据库，其数据利用率的基准为 40%，而某时间段其利用率突然上升为 99%，则说明系统中可能正在发生着针对数据库的入侵，该事件就应该被立刻报告给系统管理员。相反，有些严重程度相对较弱的事件就可以简单的记录，供日后进行审阅。

3．简化数据

日志记录的一个常见错误就是为避免错过任何细节而存储大量数据。因此，日志记录的一个基本原则是尽可能缩小日志记录的范围从而缩减日志记录的数据和日志分析所用的时间。但事实上，在很多环境中是很难做到这一点的。作为安全分析员，要利用一些数据缩减工具来缩小日志记录范围。

这些数据缩减工具通常已经被嵌入在建立系统日志的安全工具之中。CheckPonit 的 Firewall-1 的渗透保护程序就带有日志记录功能。在打开阅览器时，会呈现出所有的日志记录数据，这些数据量是相当大的，要一一审阅难度很大。CheckPoint 提供了一种过滤

技术，允许系统管理员通过使用工具快速缩减日志数据，只留下相关数据。例如，如果上周四某 SMTP 服务器遭受了邮件欺骗攻击，管理员希望将该事件记录独立的分离出来，可以建立两个过滤器来实现：一个服务器用于过滤通过 25 端口的 TCP 流量记录，一个服务器用于过滤发生在上周四的所有流量记录。这样可以有效降低日志分析工作。

16.3 系统日志安全维护

系统日常维护对系统安全也很重要。如果一个入侵者可以获得管理员权限，就可以进入系统删除相关的安全日志，进而消除其进入系统的痕迹或证据。因此，对系统日志的安全管理也必须给予高度重视。避免入侵者修改系统日志的方式主要有以下几种。

- **远程记录** 建立一个核心数据库，用于存储网络中所有系统的安全日志，该数据库的安全性必须足够高，能够防止入侵者随意修改日志记录。因此，数据库的数据都应该是只读的，其他系统只能写入数据而无法删除数据。
- **记录实时输出** 该机制一般用于较高安全性环境，打印机可以实时输出日志内容，便于日后调查。
- **机密技术** 该技术通常用于对日志文件的认证，在一个日志文件完成记录后，系统会对其进行数字签名。管理员想要审阅日志文件时，首先需要对数字签名进行认证，若认证没有通过，则说明该文件已经被修改。

16.4 系统安全审计

安全审计是安全专家必须承担的一份责任。进行审核时，安全专家分析各个系统、应用程序和整个网络的安全态势，找到其中存在的缺陷，然后制订一个行动计划解决该缺陷。

16.4.1 审计小组

实施一次成功的安全审计，最为重要的因素就是有一个受过良好训练并积极工作的审计小组。该小组成员应该由组织中最出色的安全专家组成。同时，小组成员应该包括多种职业角色，除了专业技术人员，还应该包括具有审计技术的会计师，提供业务监督、人员管理的管理人员等。如何选择小组成员取决于组织的复杂性及具体的信息安全审计要求。

16.4.2 审计工具

审计小组在进行信息安全审计时，可以利用一系列具有审计功能的工具。这些工具包括审计过程中的任务列表，用于探测系统漏洞的漏洞评估工具等。在下面内容中，将介绍几种常见的审计工具。

1. 检验表

检验表提供了一种简单的途径将组织中重复的工作标准化。检验表主要分为以下几种。

- **审计检验表** 在执行安全审计时提供适当的高级别指导，有几种不同的工作方式。
- **设置检验表** 提供网络系统设置的具体信息，通常包括由组织安全策略决定的具体设置及各种软件在系统中应发挥的作用。
- **漏洞检验表** 包括一个关键漏洞列表，这些漏洞都需要审计者在执行安全审计时进行检查。漏洞检验表的内容包括操作系统的常见漏洞和软件程序中的常见漏洞。

每种检验表在审计过程中都起到了重要作用。设计合理的检验表可以帮助系统管理员在信息安全审计中发挥重要的作用。

2. IP 和端口扫描

IP 扫描和端口扫描器是入侵者寻找系统漏洞的两个重要工具。首先通过 IP 探测确定网络中运行的系统，然后进一步探测发现开放的端口及服务。有些服务可能包含漏洞，入侵者们就通过这些数据对系统进行恶意攻击。安全管理者同样可以利用这些扫描器检测在网络中运行的流氓系统和服务。

3. 漏洞扫描

漏洞扫描器分析系统中常见的漏洞，并将其汇总起来形成详细的报告，同时给出相应的补救方法。

第一个漏洞扫描器叫做 SATAN，发布于 20 世纪 90 年代早期。SATAN 根据漏洞库中的漏洞对网络中的主机进行扫描，之后向用户提供该主机可能存在的漏洞，以便主机修复。目前最新的漏洞扫描工具叫做 SARA，在 SATAN 的基础上增加了一些新的功能，能够将存储日志记录的数据库整合在一起，便于日后分析。

一般来说审计工具的工作分为 4 个步骤。

（1）搜索网络中工作的所有主机。

（2）对这些主机进行扫描，找出主机系统开放的端口中提供的服务。

（3）分析这些服务的漏洞。

（4）根据这些漏洞提出修补意见。

4. 完整性检验

另一个用于安全审计的工具是文件完整性检验，这类工具通过密码签名技术对系统中每一个受保护的文件进行数字签名来提供完整性保护。之后周期性地扫描这些文件，重新计算数字签名，然后与数据库中存放的正确数字签名对比，若不匹配，那么就向系统管理员报告该情况。

Tripwire 是目前最为常见的完整性检验工具，以高度自动化的方式进行上述操作，

一般用于保护静态网站或其他存放核心数据的类似系统。

5. 渗透测试

上述几种工具的运行并不会影响系统的运行，只是识别系统漏洞并进行报告。寻找更多安全审计方法的安全专家提出了渗透测试，用系统化的方式对系统安全防御进行渗透，从而检测系统当前的安全态势。

执行渗透测试的人员必须是受到良好安全训练的安全专家，需要对信息安全有更好的理解，这样才能更加有效地进行渗透测试。

16.4.3 审计结果处理

审计完成以后，整个工作还没有结束，应该重新审阅整个网络系统所使用的安全技术带来的结果。事后审计的工作计划包括以下几个步骤。

（1）给出审计结果的报告，包括检测出的系统存在的缺陷及相关的详细资料。

（2）对系统面临的危险按优先级进行排列。

（3）为每个威胁提出修补意见与方案。

（4）按照优先级处理这些威胁。

（5）对修补过程进行持续性的监控，并吸取相关的经验与教训。

（6）对系统进行周期性的审计，识别系统新出现的安全威胁。

习　题

一、选择题

1．目前 Web 服务安全的关键技术有 WS-Security 规范、XML 签名规范、XML 加密规范以及下列哪一项？（　　）

A．SAML　　B．SOAP

C．XKMS　　D．OASIS

2．以下哪个方面不是检验表的主要用途？（　　）

A．远程检验表　　B．漏洞检验表

C．设置检验表　　D．审计检验表

二、问答题

1．简述日志记录的设置策略。

2．简述日志数据具体的两个操作。

3．思考如何通过通用的审计工具和技术来管理系统安全审计。

第 17 章　应用开发安全技术

本章学习重点：

- 理解数据库安全技术的概念及安全体系，掌握数据库安全的主要技术
- 了解软件存在安全问题的原因，掌握软件开发的安全模型及策略
- 理解电子商务安全策略
- 掌握 Web 安全策略

17.1　数据库安全技术

17.1.1　数据库系统面临的风险

数据库是按照数据结构来组织、存储和管理数据的仓库。随着信息技术的飞速发展，数据管理不再仅是存储和管理数据，而转变成用户所需要的各种数据管理的方式。数据库系统在实际应用中也存在来自于各方面的安全风险，这越来越引起用户和数据库生产商的注意。这些安全风险主要分为 4 类，见表 17-1。

表 17-1　数据库系统面临的主要风险

风险类型	描述
操作系统的风险	指宿主操作系统层面上的风险，数据库系统的安全性最终要靠硬件设备和操作系统所提供的环境来支撑，如果操作系统允许用户直接存取数据库文件，则在数据库系统中采取最可靠的安全措施也是没有意义的
管理的风险	主要指数据库管理部门的安全意识，对信息网络安全防范的重视程度及相关的安全管理措施等
用户的风险	主要表现在用户账号和对特定数据库对象的操作权限上
数据库管理系统内部的风险	主要指数据库管理系统自身设计等方面的缺陷与漏洞

17.1.2　数据库系统安全

1. 数据库系统安全的含义

数据库系统安全有两层含义。①系统运行安全。系统运行安全通常受到各种威胁，如一些网络不法分子通过网络等手段入侵计算机使系统无法正常启动或其他破坏硬件的活动，导致系统不能正常提供各种服务；②系统信息安全，指保护数据库以防止非法用户的越权使用、窃取、更改或破坏数据，如黑客经常入侵数据库盗取各种敏感资料等。

数据库安全除依赖自身内部的安全机制外，还涉及很多层面，如外部网络环境、应用环境、操作人员和管理人员的业务素质水平等。因此，从广义上讲，数据库系统的安全性涉及以下 3 个方面。

- **网络系统安全** 这是数据库的第一道安全屏障，数据库面向网络用户提供各种信息服务，其安全首先依赖于网络系统。数据库系统要想发挥其强大的作用离不开网络系统的支持，数据库系统的用户（如分布式用户）也要通过网络才能访问数据库。因此，可以说网络系统是数据库应用的外部环境和基础。目前，网络系统面临的主要威胁有网络欺骗、木马程序、入侵和病毒等。
- **宿主操作系统安全** 操作系统是数据库系统的运行平台。操作系统的安全策略和安全管理策略能为数据库系统提供某种程度上的保护。这些安全策略用于配置计算机的安全设置，如密码策略、审核策略、账户权利分配等。
- **数据库管理系统安全** 不同的数据库管理系统采用不同的安全设置策略。SQL Server 的安全配置经常包括：使用安全的密码策略，使用安全的账号策略，加强数据库日志的管理，使用协议加密，采取一些防注入措施等。而 Oracle 也有一些数据库安全产品，如 DBCoffer 就是一款 Oracle 数据库安全加固系统，该产品能够实现对 Oracle 数据的加密存储、增强权限控制、敏感数据访问的审计等。

这 3 个方面构筑成数据库的安全体系，与数据安全的关系是紧密相连，防范的重要性也逐层加强。

2. 数据库系统安全的特征

数据库系统的安全性主要是针对数据而言的，主要涉及 5 个方面，即数据独立性、数据安全性、数据完整性、并发控制、故障恢复。

（1）数据独立性

数据独立性包括两个方面：物理独立性和逻辑独立性。

- **物理独立性** 指用户的应用程序与存储在磁盘上的数据库中的数据是相互独立的，即应用程序要处理的只是数据的逻辑结构，而不需了解数据在磁盘上是如何存储的，数据的物理存储由 DBMS 管理，当数据的物理存储改变了，应用程序不用改变。
- **逻辑独立性** 指用户的应用程序与数据库的逻辑结构是相互独立的，当数据的逻辑结构发生改变时，用户程序也可以不用改变。

（2）数据安全性

数据存储的安全性是指数据库在系统运行之外的可读性。相比较操作系统中的对象而言，数据库支持的应用要求更为精细。为保证数据安全性，通常采取以下方法。

- 采取隔离措施，将数据库中需要保护的数据与其他数据分隔开来。
- 采取授权措施或采用访问控制方法。
- 采用数据加密技术对数据进行加密。

（3）数据完整性

为了防止数据库中存在不符合语义规定的数据和防止因错误信息的输入输出造成无效操作或错误信息，数据完整性概念应运而生，它包括数据的正确性、有效性和一致性。

- ❑ **正确性**　指数据的输入值要与数据表对应域的类型一致。
- ❑ **有效性**　指数据库中的理论数值应该满足现实应用中对该数值段的约束。
- ❑ **一致性**　指不同用户使用的同一数据应该是一样的。

数据完整性分为 4 类：实体完整性、域完整性、参照完整性和用户定义完整。可以采用外键、约束、规则和触发器等方法保证数据的完整性。

（4）并发控制

当多个事务同时存取数据库中同一数据时，数据库管理系统采取并发控制来确保数据库的完整性和统一性。例如，当某一用户对某个数据进行修改而未存入数据库时，如有其他用户也读取此数据，那么读取的数据就是不正确的。这时就需要实施并发控制，排除和防止此类错误的发生，保证数据的正确性。简单地说，并发控制的目的就是保证一个用户的工作不会影响另一个用户的工作。并发控制有多种技术手段，如封锁、时间戳、乐观并发控制和悲观并发控制等。

（5）故障恢复

数据库故障恢复和并发控制一样，都是数据库数据保护机制中的一种完整性控制。任何系统都避免不了发生故障，这就要求数据库管理系统要有一套故障恢复机构，能及时发现故障和修复故障，从而防止数据被破坏，保证数据库能够恢复到一致的、正确的状态，尽可能地减少故障带来的损失。数据库管理系统中恢复机制的核心是保持一个运行日志，记录每个事务的关键操作信息，比如更新操作前后的数据值。

17.1.3　数据库系统安全防范技术

在了解了数据库系统存在的各种风险及数据库系统安全特征之后，这里主要讨论数据库系统的安全防范技术，主要的防范技术分为下列几种。

1．物理安全

数据库系统安全防范中最基本的就是保证物理安全。这主要是指保证数据库系统在硬件、所处环境、网络连接等方面的安全不受自然或人为的破坏。比如：数据库服务器所处环境的温度、湿度是否适宜；是否只有数据库系统管理员能在物理上接触服务器等。

2．访问控制

访问控制是指数据库管理系统内部按用户身份及其所归属的某项定义组来对已经进入系统的用户的控制，或限制对某些功能的使用。它包括账号管理、密码策略、权限控制和用户认证等，主要是从账号相关的方面来保证数据库系统的安全，是数据库系统基本安全的核心。通常采取两种方法进行访问控制：①按系统模块对用户授权，即针对模块对不同用户设立不同的访问权限；②将数据库系统权限赋予用户，即用户访问数据库系统时需要进行身份认证以确认用户是否被授权访问。

3．数据加密

时至今日，利用密码技术对信息进行加密仍然是计算机系统对信息进行保护的一种

比较可靠的方式。对数据库系统中存储的重要数据进行加密，实现信息隐蔽，从而起到保护数据信息安全的作用。数据加密后，数据库表中存储的是加密后的信息，即“密文”，只有采取对应解密算法后，才能获取原始的数据信息，即“明文”。

4. 防注入技术

现在比较流行的 SQL 注入就是利用数据库的外部接口对 SQL 数据库进行查询、更新等操作，黑客可以利用此方法把用户数据插入到实际的数据库操作语言当中，从而达到入侵数据库系统甚至整个操作系统的目的。为了尽可能地保护数据库系统不受注入的攻击，可以采取相应的方法，如拒绝来自 1443 端口的探测、更改 SQL Server 默认的 1443 端口、对网络连接进行 IP 限制等。

5. 数据备份

有计划的数据备份是保护数据安全的有效手段。在数据库系统遭到破坏（误操作或者恶意攻击）后，通过恢复数据资源能尽可能地减少数据损失。SQL Server 的备份和还原组件能从多种故障中（如媒体故障、用户错误、服务器丢失等）恢复和还原存储在数据库中的关键数据。用户可以根据自己的实际情况确定数据的可用性要求，制订合适的数据库备份策略。

数据库系统的安全与网络安全、操作系统安全以及数据库管理系统安全是紧密结合的。因此，必须根据实际情况和安全需求进行分析，制订安全管理策略并进行彻底测试以确保它们实际可用。此外，还需为数据库系统管理员和用户制订相应的安全培训计划，以保证安全策略在实施过程中的有效执行。

17.2 软件开发安全技术

17.2.1 软件安全问题原因

软件安全是目前信息安全领域最为关注的问题之一。软件安全问题的原因可以分为两种：内因和外因。内因主要是指在设计过程中不可避免的缺陷以及在实现过程中的故障；外因主要是指软件运行的环境。

软件的安全问题主要包括以下几个方面。

1. 输入验证和表示法

输入验证和表示问题由元字符、替换编码、数字表示法引起。如果选择使用输入验证，那么就要使用白列表而不是黑列表。由于轻信输入而造成的问题有缓冲区溢出、跨站脚本攻击、SQL 注入、缓存毒药等。

2. 滥用 API

API 指明了调用者和被调用程序之间的使用约定。滥用 API 的常见模式是调用者错

误地信任被调用方。例如，调用者希望从被调用程序那里返回用户信息，而被调用程序并没有任何安全性保证其信息的可靠性。于是调用者就假定了调用程序返回数据的正确性和安全性。当然，也存在攻击者有意破坏调用者和调用程序之间约定的行为。

3. 安全特性

世界上所有的加密算法都不能满足真正的安全需要。认证、访问控制、机密性保障、加密算法、权限管理等都可能存在一定的安全缺陷。

4. 时间与状态

分布式计算与时间和状态相关。为了使多个组件进行通信，状态必须在组件之间共享，而所有这些都需要花费时间。因此在时间和状态之间可能存在着巨大的、未发现的天然攻击资源。

5. 错误处理

如果想破坏软件，可以让它抛出一些垃圾数据，然后看看出现了哪些错误。在现代面向对象系统中，异常的概念取代了被禁止的 goto 概念。与错误处理相关的安全缺陷在开发中很常见。在 API 被滥用的情况下，安全缺陷主要存在两种方式：①开发者忘记处理错误或者粗略地处理错误；②在产生错误时要么给出过于详细的信息，要么错误过于太具放射性以至于没有可处理它们的方式。

6. 代码质量

如果可以完整地描述系统和其存在的正面、负面的安全可能性，那么安全就成了可靠性的子集。劣质代码将导致无法预期的行为，从软件使用者的观点，它的可用性是很差的；而从攻击者的角度看，糟糕的代码将提供给系统施压的可乘之机。

7. 封装

封装是指在事物之间的边界和它们之间建立的界限。在 Web 浏览器中，它确保了移动代码不能够强行攻击硬盘。在 Web 服务端，它意味着在经过认证的有效数据和私密数据之间的差别。这里的边界非常重要，如今在类之间的一些方法构成了重要的边界，因此信任模式需要谨慎地设置。

8. 环境

环境指上述内容的外部领域，包括在代码外部的所有东西，它也是软件安全领域不可忽视的问题。

17.2.2 软件安全开发模型

目前，软件安全开发主要有两种模型：一种是微软公司的安全开发模型——安全开发生命周期模型（SDL）；另一种是威胁建模模型。

1. 安全开发生命周期

安全开发生命周期模型分为以下 4 个步骤。

（1）对不同人群进行安全教育，从而提高安全意识。

- **设计人员** 学会分析威胁。
- **开发人员** 跟踪代码中每一字节的数据，质疑所有关于数据的假设。
- **测试人员** 关注数据的变化。

（2）设计阶段，利用威胁建模技术建立系统模型。

（3）开发阶段，编码与测试并行。

（4）发行与维护阶段，使用标准的修复机制修复安全缺陷。

2. 威胁建模

威胁模型是一种基于安全的分析，有助于人们确定给产品造成最高级别的安全风险，以及攻击是如何表现出来的。其目标是确定需要缓和哪些威胁及如何缓和这些威胁。威胁建模主要分为以下 4 个步骤。

（1）分解应用程序。使用数据流图（DFD）或统一建模语言（UML）描述威胁模型作为分析应用程序的重要组成部分。对应用程序进行形式化分解，自顶向下、逐层细化，在分解过程中关注过程之间的数据流。

（2）确定系统面临的威胁。按照“STRIDE”威胁模型来分类，见表 17-2。

表 17-2 “STRIDE”威胁模型

威胁类型	描述
S	Spoofing identity，即身份欺骗，冒充合法用户、服务器进行欺骗（DNS 欺骗，DNS 缓存中毒）
T	Tampering with data，篡改数据
R	Repudiation，否认
I	Information disclosure，信息泄露
D	Denial of service（DOS），拒绝服务
E	Elevation of privilege，特权升级

（3）威胁评估。按照“DREAD”算法为威胁分级（表 17-3），并建立攻击树。

表 17-3 “DREAD”威胁等级

威胁等级	涵义	威胁等级	涵义
D	Damage potential，潜在的破坏	A	Affected users，受影响的用户
R	Reproducibility，再现性	D	Discoverability，可发现性
E	Exploitability，可利用性		

例如：

- **Threat #1** 恶意用户浏览网络上的秘密工资数据。
- **潜在的破坏性** 读取他人的私密工资并不是开玩笑的事——风险值为 8。

- **再现性** 100%可再现——风险值为10。
- **可利用性** 必须处于同一子网或者处于同一路由器下——风险值为7。
- **受影响的用户** 每个人都将受到影响——风险值为10。
- **可发现性** 假设它已经发生——风险值为10。
- **计算风险 DREAD** (8+10+7+10+10) / 5 = 9。

攻击树描述了攻击者利用系统漏洞破坏各组件，对威胁目标进行攻击所经历的决策过程。建立攻击树需要考虑以下几个方面。

- **安全威胁** 潜在的事件，当攻击有动机并付诸实施时，威胁转变为攻击事件。
- **安全漏洞** 系统中的弱点。
- **资源** 受威胁（或攻击）的目标。

（4）建立缓和方案，选择适当的安全技术。

17.2.3 软件安全开发策略

在软件开发的不同阶段实施相应的安全开发策略。

1．规划体系结构和设计解决方案

（1）识别和评估威胁：使用威胁建模系统地识别威胁，而不是以任意的方式应用安全性。接着根据攻击或安全损害产生的风险和可能造成的潜在损失，对威胁进行评估，这样就可以适当的次序对威胁进行处理。

（2）创建安全的设计：使用尝试或检验过的设计原则。集中处理关键区域，在这些区域，经常会出现错误，这里称之为应用程序缺陷类别。其中包括输入验证、身份验证、授权、配置管理、敏感数据保护、会话管理、密码系统、参数处理、异常管理和审核与日志记录各项。要特别注意部署问题，包括拓扑、网络基础设施、安全策略和步骤。

（3）执行体系结构和设计复查：应用程序设计的复查与目标部署环境和相关的安全策略有关。需要考虑底层基础设施层安全性（包括边界网络、防火墙、远程应用程序服务器等）带来的限制。使用应用程序缺陷类别对应用程序进行分类，并分析适合于每个领域的方法。

2．进行应用开发

（1）开发工具的安全性：充分了解开发工具（包括语言、虚拟机、IDE 环境、引用的第三方工具包等），最好选择开放源代码的开发工具，这样可以更好地审核其安全性。检查开发工具是否提供了用户和代码安全模型，是否允许对用户和代码可以执行的操作进行限制。如果开发中涉及公开对称和不对称的加密与解密、散列、随机数生成、数字签名支持等算法，最好选用可靠的公开算法，避免自己炮制算法。

（2）编写安全代码库：对程序集进行数字签名，使它们不能被随意改动。通过遵守面向对象设计原理，减小程序集的受攻击面，然后使用代码访问安全性，进一步限制哪些代码可以调用您的代码。使用结构化的异常处理方法防止敏感信息蔓延到当前信任边界之外，并开发更加可靠的代码。避免常规问题，特别是输入文件名和 URL 的问题。

（3）安全地处理异常：不要显示内部系统或应用程序的详细信息，如堆栈跟踪、SQL语句片断等。确保这类信息不被允许蔓延到最终用户或当前信任边界以外。在异常事件中安全地“失败”，确保应用程序拒绝非法访问，而且没有停留在不安全的状态下。不记录敏感或私有数据，如密码，以免造成危害。在记录或报告异常时，如果用户的输入包括在异常消息中，需对其进行验证或清理。例如，如果返回一个 HTML 错误消息，那么应该对输出进行编码，以避免脚本注入。

（4）执行第三方代码的安全复查：使用分析工具分析二进制程序集，确保它们符合安全设计准则，并修复分析工具识别出的所有安全缺陷。复查具体的应用程序元素，包括 Web 页面和控件、数据访问代码、Web 服务、服务组件等。此外，要特别注意 SQL 注入和跨站点脚本编写缺陷。

（5）保证开发人员工作站的安全性：使用一套方法保证工作站的安全性。保证账户、协议、端口、服务、共享、文件与目录和注册表的安全。最重要的是，保持工作站具备当前最新的补丁与更新。例如，如果要在 Windows XP 或 Windows 2000 上运行 Internet 信息服务(IIS)，则运行 IISLockdown。IISLockdown 应用安全的 IIS 配置，并安装 URLScan Internet 安全应用程序编程接口（ISAPI）筛选器，该筛选器用于检测和拒绝潜在的恶意 HTTP 请求。

（6）编写具有最低权限的代码：可以限制代码能够执行的操作，这与运行该代码所使用的账户无关。通过配置策略或编写代码，可以使用代码访问安全性控制来限制代码允许被访问的资源和操作。如果代码不需要访问某种资源或执行某种敏感操作，可以通过安全性配置来确保代码不会被授予这种权限。

（7）防止 SQL 注入：使用数据访问的参数化存储过程。使用参数要确保输入值的类型和长度都得到检查。将参数视作安全文本值和数据库内的不可执行代码。如果不能使用存储过程，也可以使用带有参数的 SQL 语句，但不要通过连接 SQL 命令和输入值来构建 SQL 语句。此外，还要确保应用程序使用具有最低权限的数据库登录，以限制它在数据库中的功能。

（8）防止跨站点脚本编写：对输入类型、长度、格式和范围进行验证，并对输出进行编码。如果输出包括输入（包括 Web 输入），则对输出进行编码。例如，对窗体字段、查询字符串参数、cookie 等进行编码，以及对从无法确定其数据是安全的数据库（特别是共享数据库）中读取的输入进行编码。对需要以 HTML 返回客户端的自由格式的输入字段，对输出进行编码，然后选择性地清除在许可元素上的编码。

（9）管理机密：最好寻找避免存储机密的替代方法。如果必须存储它们，则不要在源代码或配置文件中以明文的方式存储。

（10）安全地调用代码接口：特别注意传递给接口和接口返回的参数，防止潜在的缓冲区溢出。验证输入和输出字符串参数的长度，检查数组边界及文件路径的长度。

（11）执行安全的输入验证：对输入进行限制、拒绝和清理，因为验证已知有效类型、模式和范围的数据要比通过查找已知错误字符来验证数据容易得多。验证数据的类型、长度、格式和范围，对字符串输入，则使用正则表达式。有时候可能需要对输入进行清理，如在对数据编码后清理编码元数据，以保证其安全性。

（12）保证页面访问身份验证的安全性：安全地划分 Web 站点，隔离匿名用户可以

访问的公共可访问页面和需要身份验证访问的限制性页面。使用安全套接字层（SSL）来保护窗体身份验证凭据和窗体身份验证 cookie。限制会话生存时间和确保身份验证 cookie 只在 HTTPS 上传输。对身份验证 cookie 加密，不要在客户端计算机上保留它，也不要将其用于个性化目的；对个性化使用单独的 cookie。

3. 管理和维护系统

（1）实现补丁管理：针对 Microsoft 平台，那么可以使用 Microsoft Baseline Security Analyzer（MBSA）来检查当前可能漏掉的补丁和更新。定期运行该操作，保持服务器当前安装有最新的补丁和更新。在应用补丁前，对服务器数据进行备份；在将补丁安装在生产服务器上之前，先在测试服务器上进行测试。还要使用 Microsoft 提供的安全通知服务，并订阅通过电子邮件接收的安全布告。针对 UNIX/Linux 平台，可以订阅有关漏洞及补丁的邮件列表，定期使用工具，检查服务器上安装的补丁是否与 UNIX/Linux 厂商发布的最新补丁列表相一致。

（2）保证 Web 服务器的安全性：针对 Microsoft 平台上运行的 IIS 服务，可以使用 IISLockdown 应用安全的 IIS 配置，并安装 URLScan Internet 安全应用程序编程接口（ISAPI）筛选器，该筛选器用于检测和拒绝潜在的恶意 HTTP 请求。针对 UNIX/Linux 平台上运行的 Apache 服务，可以采用选择性访问控制（DAC）和强制性访问控制（MAC）的安全策略，或者安装安全相关的模块。针对 WebService 常用的协议（如 soap），可以使用 XML 加密以确保敏感数据保持其私有性。使用数字签名保证消息的完整性，特别重要的数据应使用 SSL 加密。最重要的是，保持服务器安装了当前最新的补丁和更新，并使其按照最小权限运行。

（3）保证数据库服务器的安全性：应用一种常见方法评估账户、协议、端口、服务、共享、文件与目录和注册表。还要评估 SQL Server 的安全设置，如身份验证模式和审核配置。评估身份验证方法和 SQL Server 登录、用户与角色的使用。确保安装最新的服务包，定期监测操作系统和 SQL Server 补丁与更新。

（4）防止拒绝服务攻击：确保加强了服务器上的 TCP/IP 堆栈配置，以应对如 SYN flood 这样的攻击。对 Web 服务的配置做适当的修改以限制接受的 POST 请求的规模，并对请求的执行时间做出限制。

（5）限制文件 I/O：可以配置代码访问安全策略，以确保限制单个程序集或整个 Web 应用程序只能访问文件系统。例如，通过配置运行在媒体信任级上的 Web 应用程序，可以防止应用程序访问其虚拟目录层次结构以外的文件。同时，通过为特定程序集授予受限的文件 I/O 权限，可以精确控制哪些文件可以被访问以及应该如何访问它们。

（6）执行远程管理：针对 Microsoft 平台，其终端服务提供了一种专用的协议（RDP）。它支持身份验证，并提供加密。如果需要文件传输工具，可以从 Windows 2000 Server 资源包中安装文件复制实用工具。建议不要使用 IIS Web 管理，如果运行 IISLockdown 该选项将被清除。应该考虑提供一个加密的通信通道，IPSec 限制可以远程管理服务器上的计算机。还应该限制管理账户的数量。针对 UNIX/Linux 平台，建议采用 SSH 进行远程管理，文件传输使用 SFTP。

17.3 电子商务安全策略

17.3.1 电子商务安全基础

电子商务是一个不断发展的概念，通常指以商务活动为主体，电子化方式为手段，互联网为基础和工具的各种商业活动、贸易活动、金融活动和其他相关综合服务活动的一种商业运营模式。安全性始终是电子商务的核心和关键问题，也是制约其发展的最重要因素。如何建立一个安全的电子商务应用环境，保证整个商务活动中信息的安全性和交易者的利益已经成为一个重要话题。

1. 电子商务的安全要求

电子商务的一个重要特征就是利用计算机技术、网络技术和远程通信技术来处理和传输商业信息，而由于互联网本身的开放性特点，使得网上交易面临种种威胁，常见的威胁如下。

（1）虚假身份的交易对象及虚假合同、订单。

（2）商业机密在传输过程中被第三方获取、泄露、篡改或恶意破坏。

（3）交易对象的抵赖。

（4）信息破坏，只要指由计算机系统或网络故障造成的对交易过程和商业信息安全的破坏等。

因此，为了保证电子商务过程能够安全顺利地完成，电子商务的信息安全有以下几点安全控制要求。

（1）信息的保密性

电子商务作为贸易的一种手段，其信息一般都直接涉及到交易者的商业机密。保证商业机密安全是电子商务安全的重要内容。因此，为了预防信息在交易过程中被非法窃取，交易中的商务信息均有保密要求。保密性一般通过密码技术对传输的信息进行加密处理来实现。

（2）信息的完整性

信息的完整性包括信息在电子商务交易过程中不被篡改和破坏，以及在传输的过程中保证收到的信息和原发送的信息的一致性。保持贸易各方信息的完整性是电子商务应用的基础。输入数据可能出现的意外差错或者欺诈行为都会导致交易各方信息的差异，因此为了维护商业信息的完整和统一，电子商务系统应该充分保证数据传输、存储及电子商务完整性检查的正确性和可靠性。一般使用信息摘要的方式来保持信息的完整性。

（3）信息的真实性

信息的真实性是保证电子商务顺利实现的基础，它包括两方面：一是指网上交易双方提供信息内容的真实性；二是指交易双方身份的真实性，而非假冒或者不存在的。为了保证身份的真实性，使交易双方能够在互不见面的情况下完成交易，需要对人或实体的身份信息进行鉴别和认证，这通常由认证机构和证书来实现。

（4）信息的有效性

交易信息的有效性是电子商务顺利完成的前提。电子商务的交易信息以电子形式存在而不同于传统的纸张模式，其有效性直接关系到交易者的经济利益和声誉，因此要对各种潜在的威胁，诸如操作错误、网络故障、软硬件故障、病毒与木马等加以控制和预防，确保交易信息在确定的时刻和确定的地点是有效的。

（5）信息的不可否认性

交易信息的不可否认性是交易过程严肃和公正的体现，它是指交易一旦达成是不能被否认的，交易信息是不可被修改的，即任何一方不能否认已经确认完成的交易过程，否则必然会给另一方带来损失。由于交易方式的特殊性，在电子商务中通过手写签名和印章进行交易双方的鉴别已经不可能，因此必须在交易信息的传输过程中为交易者提供可靠的标识。

2. 电子商务安全技术

电子商务是以互联网的基础设施和标准为基础，涉及电子技术、计算机技术、通信技术等广泛领域。为了保证电子商务整个过程的安全顺利执行，一些安全技术和安全机制被运用到电子商务中。

（1）防火墙技术

防火墙是建立在内外网络边界上的过滤封装机制，它负责过滤进入或离开计算机网络的通信数据，通过对接收到的数据包和防火墙内部过滤规则库中的安全规则进行比较，决定是否把一个数据包转发到它的目的地。防火墙有两种安全策略：未被允许访问的服务都是被禁止的；未被禁止访问的服务都是允许的。目前使用的防火墙主要可分为包过滤型和状态检测型两种。

防火墙技术是网络安全中最重要的安全控制技术。简单防火墙技术可以在路由器上实现，而专用防火墙可以提供更加可靠的网络安全控制。但是，防火墙仅是复杂的边界保护链中的一环，而且自身也有一定的局限性，所以还需要其他安全技术配合使用。

（2）数字加密技术

数字加密被认为是网络中最基本的安全技术，也是电子商务中最基本的安全保障形式。它是通过加密算法对敏感信息进行加密，然后把加密好的数据（密文）和密钥在线路上传送给接收方或者在数据库中存储，接收方只有通过解密算法对密文进行解密才能获取敏感信息，从而保证了数据的机密性。

数字加密技术有两类最基本的方法：对称加密技术和非对称加密技术。在对称加密技术过程中，加密和解密算法使用相同的密钥，其特点是加解密速度快、保密性强，但前提是必须通过安全的途径来传送密钥。典型的对称加密算法有 DES 和 IDEA。而非对称加密技术则是使用一对在数学上相互关联的密钥：一个公开密钥和一个私有密钥。从公钥推导出密钥需要超大的计算量，实际上是不可行的。非对称加密的特点是可以适应网络开放性要求，且密钥管理问题相对简单，但是算法复杂，加密速率相对较低。典型的非对称加密算法有 RSA 算法。

（3）认证技术

安全认证技术是保证电子商务活动中的交易双方身份及其所用文件真实性的必要手

段，它包括数字摘要技术、数字签名技术、数字时间戳技术、数字证书和生物识别技术等。

- 数字摘要就是采用单向 Hash 函数将任意长度的消息“摘要”成固定长度的（128 位）摘要信息串。不同的输入信息产生的摘要信息必定不同，而相同的输入信息产生的摘要信息必定相同。数字摘要技术可以保证数据的完整性。
- 数字签名是指以电子形式存在于数据信息之中，或作为其附件，或逻辑上与之有联系的数据，用来辨别数据签署人的身份及其对所含信息的认可。数字签名技术是不对称加密算法的典型应用，它能保证信息传输的完整性、发送者的身份认证，防止交易中的抵赖发生。
- 数字时间戳是服务（Digital Time-stamp Service，DTS）是由 DTS 服务机构提供的专门用于证明信息发送时间的电子商务安全服务项目。数字时间戳的过程为：用户首先将需要加时间戳的文件用 Hash 算法形成信息摘要并发送到 DTS，DTS 在加入了收到文件信息摘要的日期和时间信息后再对该文件进行加密（数字签名），然后送回给用户。
- 数字证书是网络通信中标志通信各方身份信息的一系列数据，它提供了一种在互联网上验证身份的方式。数字证书由一个由权威机构——CA（Certificate Authority）发行，它绑定了公钥及其持有者的真实身份，可以灵活运用在电子商务中。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。数字证书具有唯一性和可靠性特点，而且可以存储在多种介质上。
- 生物识别技术主要是指通过人类生物特征进行身份认证的一种技术，可用于政府、银行、电子商务、安全防务等领域。现阶段，常见的生物识别技术有指纹识别、手掌几何学识别、虹膜识别、视网膜识别、面部识别、签名识别、声音识别等，其中指纹识别技术已广泛运用于微型支付等电子商务领域。

（4）协议层技术

电子商务中最常见的安全机制有 SSL（安全套接层协议）及 SET（安全电子交易协议）两种。

SSL 是由 Netscape 开发的，旨在为网络通信提供安全及数据完整性的一种安全协议，它在应用程序进行数据交换前通过交换 SSL 初始握手信息来实现有关安全特性的审查。SSL 协议提供的服务主要有：认证用户和服务器，确保数据发送到正确的客户机和服务器；加密数据以防止数据中途被窃取；维护数据的完整性，确保数据在传输过程中不被篡改。但是 SSL 协议仍存在一些问题，例如只能提供交易中客户与服务器间的双方认证，在涉及多方的电子交易中，SSL 协议并不能协调各方间的安全传输和信任关系。为了实现更加完善的即时电子支付，SET 协议应运而生。

SET 协议是由美国 Visa 和 MasterCard 两大信用卡组织联合国际上多家科技机构，共同制定的应用于互联网上的以银行卡为基础进行在线交易的安全标准，它采用公钥密码体制和 X.509 数字证书标准，主要应用于保障网上购物信息的安全性。SET 协议提供了商家、消费者和银行之间的认证，确保了交易数据的安全性、完整可靠性和交易的不可否认性，它已经成为目前公认的信用卡/借记卡的网上交易的国际安全标准。

17.3.2 电子支付系统安全

1. 电子支付技术

电子支付技术必须能使收款人收到合法支付，阻止未授权支付，并保护参与者隐私。

（1）联机支付与脱机支付

大多数网上支付系统是联机支付系统，每次支付中包含一项授权服务并实时更新支付状态；但是，脱机支付在支付过程中不牵涉第三方，只涉及付款人和收款人，系统的本地状态容易被付款人重新设置为支付前的状态造成透支和欺诈。

（2）可信赖硬件

为了防止透支，脱机支付系统付款人和收款人需要安装抗干扰硬件，由一个可以信赖的保护密钥和执行必要操作的安全智能设备（即电子钱包）来确保安全。

（3）密码

安全的支付系统必须采用各种密码安全技术，一般包括4类：无密码系统、一般的支付交换设备、共享密钥密码和公开密钥数字签名。

（4）付款人匿名

付款人匿名指的是在支付时不使用支付人的身份，隐藏付款人与收款人之间的信息流，所有支付系统不能够跟踪。

电子支付系统与其他安全系统一样，必须具备五性，即授权、完整性、保密性、可用性和可靠性。一般说来，电子支付系统的特征和定义决定了其操作上的安全需求。

2. 授权与完整性

完整性支付系统要求用户必须在授权的情况才能接触进行支付，因此，授权就是支付系统中最重要的环节，它一般有3种方式：外部授权、口令和签名。

- **外部授权** 指的是授权方通过一个安全的外部通道（如邮件或电话）同意或否定支付的通用方法。
- **口令授权** 指的是由授权方和检验方通过密码检查值作为口令保护的交易方法。
- **数字签名** 指的是由检验方要求授权方进行数字签名并且提供一个原始的非拒绝支付证据的方法。

3. 保密性

电子支付系统的保密性指的是防止泄露有关交易的所有信息（如付款人和收款人的标识、交易的内容和数量等）。保密性要求这些信息只能让交易的参与者知道，甚至只能是部分参与者知道。

4. 可用性和可靠性

可用性和可靠性一般通过可靠的存储器和专用同步协议来保证基本网络服务和软硬

件系统足够可靠并且可恢复故障。交易方要求无论何时都可以进行支付交易而且是完整发生的，不能处于一种未知或不一致的状态，交易方不希望网络或系统故障导致他们的损失。

17.3.3 生物识别安全技术

生物识别技术主要是指通过人类生物特征进行身份认证的一种技术，通常具有唯一的、可测量的，可自动识别和验证的，具有遗传性或终身不变等特点。生物识别的核心就是获取生物特征并转换为数字信息存储分析，利用可靠的匹配算法验证识别个人身份。

（1）指纹识别：是所有生物识别技术中应用最为广泛的一种，由于其价格低廉、体积较小及容易整合，适用于室内安全系统特别是工作站安全访问系统。

（2）手掌几何学识别：是通过测量使用者手掌的物理特征进行识别并进行三维成像的方法。由于其性能好、使用方便、准确性非常高及调整灵活，适用于用户人数比较多的场合。

（3）声音识别：是通过分析使用者声音物理特性进行识别的技术。由于传感器和人的声音可变性很大、使用步骤复杂、在某些场合使用不方便等原因，应用范围相对受限。

（4）视网膜识别：是使用光学设备发出的低强度光源扫描视网膜特征的识别方法。由于精度要求高以及用户接受程度低等原因，目前仍然没有成为主流的生物识别产品。

（5）虹膜识别：是生物识别中对人的干扰较少的技术。由于其无须与用户接触并且存在更高的模板匹配性，虹膜扫描设备的简便性和系统集成方面优势进一步有待提升。

（6）签名识别：是一种相当准确并且可被接受的识别符，但相对来说，这类产品目前数量很少。

（7）面部识别：是一种价值很高的技术，在比较两个静态图像的基础上，动态的发现和确认某个人的身份而不引起注意，是目前比较期待的重要的生物识别方法，但实际应用中还很少成功。

（8.）基因识别：基因是代表个人遗传特性、独一无二、永不改变的指征，因此，基因识别是一种高级的生物识别技术，但由于不能做到实时取样和迅速鉴定，限制了其广泛应用。

（9）静脉识别：是一种利用近红外线读取个人的静脉模式，并与预先存储的静脉模式进行比较从而进行的本人识别。

（10）步态识别：是利用摄像头采集人体行走过程的图像序列，进行处理后与存储的数据进行比较识别身份的技术。一般用于实现远距离的身份识别和主动防御中。

现阶段中国巨大的人口基数及其越来越频繁的流动性，需要静态或动态的对身份进行识别管理和控制，频繁的身份认证需求，特别是在电子商务和电子政务中演变和普及生物识别技术，是现阶段可预见的最佳解决方案。因此，目前生物识别技术主要有三大应用方向。

（1）作为刑侦鉴定的重要手段。

（2）满足企业安全管理需求。

（3）自助式政府服务、出入境管理，金融服务、电子商务，信息安全（个人隐私保护）。

17.4 Web 服务安全技术

Web 服务技术是最近几年迅速兴起的一种应用集成技术，是一个崭新的分布式计算模型，一经推出就以它的松耦合性、跨平台性和交互性受到众多企业的支持。而 Web 服务的这些特性也引出了一些安全问题，制约了它的应用和推广发展。

17.4.1 Web 服务概述

（1）Web 服务架构

Web 服务是一系列标准和正在发展中的标准，它们是由 Worldwide Web Consortium（W3C）设计和指定的，用来促进跨平台的程序和程序之间的通信。图 17-1 描述了 Web 服务的基本架构。

该架构由 3 个参与者和 3 个基本操作构成。3 个参与者分别是服务提供者、服务请求者和服务代理，而 3 个基本操作分别是发布（publish）、查找（find）和绑定（bind）。服务提供者将服务发布到服务代理的一个目录上；当服务请求者需要调用该服务时，他首先利用服务代理提供的目录去搜索该服务，得到如何调用该服务的信息；然后根据这些信息去调用服务提供者发布的服务。当服务请求者从服务代理得到调用所需服务的信息之后，通信是在服务请求者和提供者之间直接进行，而无须经过服务代理。

（2）Web 协议体系概述

Web 服务体系使用一系列标准和协议实现相关的功能。Web 服务的协议层次如图 17-2 所示。

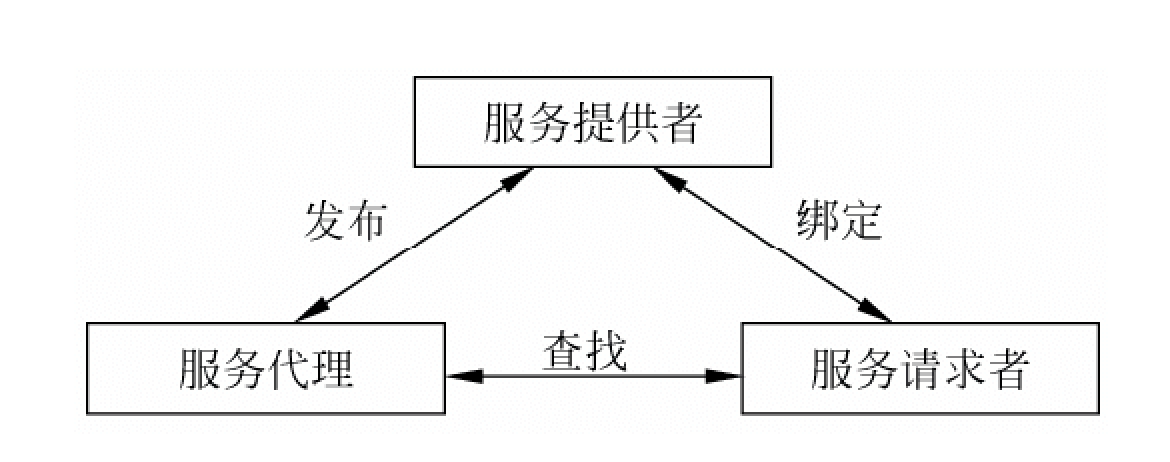


图 17-1　Web 服务架构



图 17-2　Web 服务协议层次

XML（Extensible Markup Language，可扩展标记语言）：XML 是由 W3C 创建的一种基于文本的规范标记语言，是 Web 服务平台中表示数据的基本格式。其特点是：易于理解，跨平台性，结构松散耦合，互操作性强。

SOAP（Simple Object Access Protocol，简单对象访问协议）：SOAP 为在一个松散的、分布的环境中使用 XML 对等地交换结构化信息提供了一个简单的轻量级机制。SOAP 的目的是为了使分布于网上的各系统之间能够进行数据传输。

WSDL（Web Services Description Language，Web 服务描述语言）：WSDL 提供了一个基于 XML 的简单语汇表，将 Web 服务描述为能够进行消息交换的服务访问点集合，用来描述通过网络提供的基于 XML 的 Web 服务。

UDDI（Universal Description，Discovery and Integration 统一描述、发现和集成协议）：UDDI 是一套基于 Web 的、分布式的、面向 Web 服务的信息注册中心的实现标准规范，它定义了 Web 服务的发布和发现的方法。

17.4.2 Web 服务安全

1. 传统 Web 安全技术

传统的 Web 安全技术主要集中于对网络连接和传输层的保护。通常有安全套接字层（SSL）、IP 安全协议（IPSec）、防火墙规则以及虚拟专用网（VPN）等。其中 IPSec 过滤策略和防火墙规则限制已知 IP 对服务的访问，可有效地保证数据完整性。但是根据策略和规则的设置，它只能放行或者过滤掉所有的 SOAP 消息，却无法检测 SOAP 消息的安全性。

SSL 是广泛作业于 HTTP 的安全技术。SSL 保护客户与服务器之间的通信通道，它支持客户与服务器的认证，提供了数据完整性、数据机密性和点到点的安全会话。但采用 SSL 却存在一些问题。首先，SSL 只能保证两点之间的一个连接，无法保证端对端的数据完整性、机密性。在多跳通信情况下，SSL 要求消息在每个跳之间加密解密，这不仅影响了性能，还可能损害消息的安全。其次，SSL 没有为安全应用提供足够的粒度。SSL 只能对整个文档进行加密，因此会严重影响性能。另外，SSL 还局限于传输协议，这意味着如果 Web 服务使用一个不同传输协议时，SSL 就不起作用了。

由此可见，传统安全技术无法完全满足 Web 服务的端到端安全、选择性保护等新的安全需求。Web 服务通信安全需要在应用层有效地保证 SOAP 协议在交换过程中消息的完整性与机密性，实现细粒度的消息保护。

2. 目前 Web 服务安全的关键技术

目前 Web 服务中采用的安全技术主要有以下几种：①在客户端建立用户信任机制，执行服务时将相应的认证信息导入服务器；②在 SOAP 消息头中加入针对特定应用的安全表示（token），则可从中提取认证、信任信息；③在某个特定的应用领域内，对服务提供者的内部敏感数据进行加密，当其收到服务请求后直接在加密了的数据上进行相应的计算和处理，计算结果解密后返回给服务请求者；④服务请求者需要提交必要的输入数据，并且每次仅提交一个输入数据块，返回的结果对应于该请求，经过多次服务请求后，由服务请求者进行各次服务执行结果的集成，从一定程度上保证了客户信息的安全。

为了保证 Web 安全，一些安全规范被建立并引入到 Web 安全领域中。

（1）XML 签名规范

XML 签名（XML Signature）是 IETF 和 W3C 工作组联合提出的规范。XML 签名的功能在于它既可以提供数据的完整性（Integrity），又具有鉴别性（Authentication）和不可抵赖性（Nonrepadiatability），对于保障使用计算机及网络完全有着其他办法不可替代的作用。在 XML 签名中，签名通过间接方式应用到数字内容上，要签署的内容首先将进行摘要并被放置在一个 XML 元素中，随后对元素进行摘要并秘密将其签署，签名

应用于这个摘要。由于摘要通常会比原始数据小，所以使用它可以缩减加密和签署数据时所需的时间，而这个缩减可以使数据的传输和存储更为有效。XML 签名的结构如下：

```
<Signature id?>
<SignedInfo>
(<!一规范化法则的 URI-->
<CanonicalizationMethod>
(!一数字签名算法一>
<SignatureMethod/>
<Reference/>+
</SignedInfo>)
<SignatureValuet>
<!一签署公钥或 CA-->
<KeyInfo/>
</Signature>
```

其中，<SignedInfo>，是 XML 签名的根元素，它封装了签名数据；<CanonicationMethod>，表示在进行摘要之前对<SignedInfo>元素进行规范化的算法；<SignatureMethod>，指定将规范化后的<SignedInfo>进行签名成为<SignatureValue>的算法。它由摘要算法、密钥相关的算法和一些其他算法组成；<Reference>，用于描述签名对象相关的信息，包含用来计算摘要的算法、计算后的摘要值等；<SignatureValue>，是签名处理后确切包含的签名值；<KeyInfo>，表示用于验证签名的密钥。其标识可以包括证书、密钥名称和密钥协议算法。

与传统数字签名相比，XML 签名在处理 XML 文档签名时，表现出强大的功能和技术优势。首先，XML 签名结果保持 XML 文档的结构性，便于数字签名的存储和管理。其次，XML 数字签名借鉴了 Internet 资源的 URI 建模思想，对待签名数据也用 URI 建模。URI 可以引用任意数据类型的文档，也无论是远程文档还是本地文档，甚至还可以引用 XML 文档的任意元素。因此利用 URI 不仅可以对整个 XML 文档签名，而且可以对 XML 文档的任意元素签名，实现传统数字签名无法做到的细粒度签名。另外，签名密钥表示形式的语义清晰、易读、友好，提高了签名的可移植性和自动验证能力。XML 签名的缺点是 XML 签名未能提供一个标准的编程 API 或者用于处理签名的 Web 服务模型，这使得应用程序的代码依赖于专用的供应商 API，从而消减了应用程序的可移植性。并且，在安全考虑因素中，通过转化可能会引入安全漏洞，从而使签名的有效性受损。

（2）XML 加密规范

XML 加密（XML-Encryption）是一个 W3C 的推荐标准，该规范是为数据保密性而定的，它定义了在 XML 文档中加密和解密所选元素的语义和处理规则。XML 加密并不是一种新的加密算法，以前的任何一种加密算法都可以用在 XML 加密中。XML 加密的结果就是<EncrytedData>元素，EncrytedData 元素是 XML 加密中使用的主要语法组件，其他所有 XML 加密元素都是其子元素。XML 加密的结构如下：

```
<EncryptedData Id? Type?>
<!--加密算法的 URI-->
<EncryptionMethod/>?
```

```
<!--密钥信息-->
<KeyInfo/>
<!一加密的数据内容一>
<CipherData>
<CipherValue/>
</CipherData>
<EncryptionProperties/>?
</EncryptedData>
```

其中，<EncryptedData>元素是加密数据和解密所需相关信息的最外层元素。<KeyInfo>元素是<EncryptedData>的子元素，提供用于加密和解密数据的对称会话密钥。<CipherData>元素是<EncryptedData>的必要子元素，包含或引用实际的加密数据。XML 加密提供了 SSL 未涉及到的两个重要领域：加密部分文档、实现端对端的安全。直接对文档加密，最大问题就是加密的粒度太大，这种方法在一些特殊情况下，不能满足要求并且影响效率。

XML 加密规范对加密的粒度进行了分类，可以加密整个文档或者文档的一个元素，实现了对文档的部分进行加密、以及实现传输层以外的安全。XML 加密的另一优势在于加密后的数据以 XML 格式表示，并且可以作为独立的 XML 文档而存在，因此便于存储和管理。XML 加密缺点是：加密的语法和处理模型非常复杂，将加密后的 XML 片段插入到另一个上下文中时也会出现 ID 冲突等问题。并且 XML 加密对解决某些安全问题的能力还有一定限制，而与 XML 签名结合也可能会引发新的安全问题，例如常见的明文推测攻击、拒绝服务攻击等。

SAML（Security Assertion Markup Language，安全断言标记语言）是一个 OASIS 标准，它定义了以 XML 格式交换安全信息的框架，如图 17-3 所示。

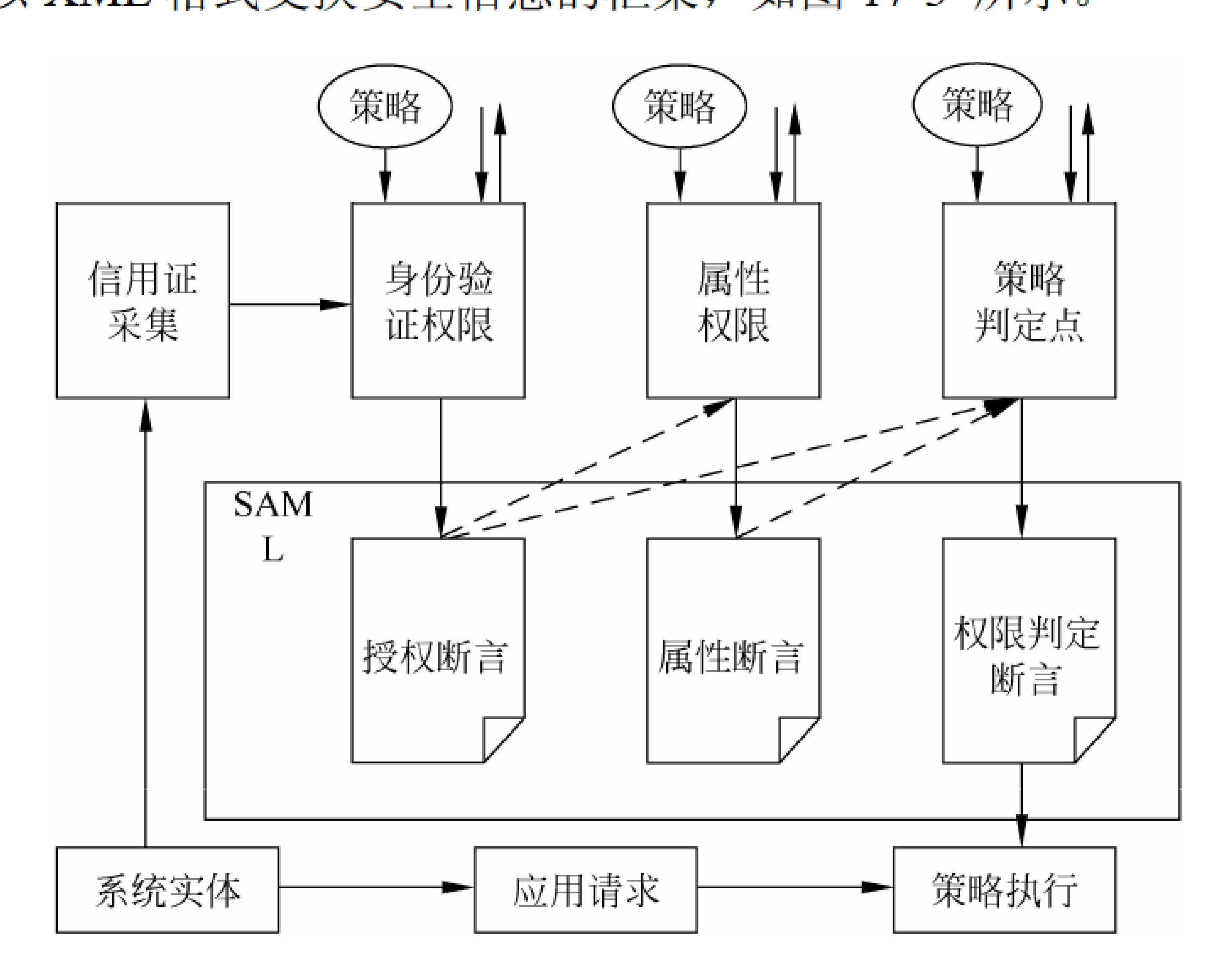


图 17-3 SAML 框架示意

安全信息包括验证设备、授权决策和主题属性，都以称为“断言”的 XML 结构进行描述，断言有 SAML 权威部门发放。SAML 规范也定义交换断言的协议、传输绑定

和使用方案，它无缝地映射到 SOAP 传输。

（3）WS-Security 规范

WS-Security 规范是 IBM Microsoft 和 VerSign 公司共同提出的一个协议规范。XML 签名和加密以及 SAML 等不是直接解决 Web 服务安全性的方法，WS-Security 解释了如何将这些技术应用到 Web 服务安全中。WS-Security 定义了在 SOAP 消息中如何包括安全令牌，以及如何使用 XML 安全规范来加密和签名这些令牌，同时也定义了如何使用它们来对 SOAP 消息的其他部分进行签名和加密，即定义了将令牌封装到 SOAP 消息中的 XML 元素和属性，以及将 XML 签名和 XML 加密封装到 SOAP 中的方法。

除以上这些安全规范外，还有一些安全技术被用来保证 Web 服务的安全。例如，XACML（XML Access Control Markup Language）是一个 OASIS 标准，定义了一个通用的授权框架和以 XML 格式表示、交换访问控制策略信息的结构。PKI（Public Key Infrastructure，公钥基础设施）为 Web 服务安全的最底层，它通过 XKMS（XML Key Management Specification）协议为 Web 服务提供了基础的 XML 公钥系统 PKI，即 XKMS 是给 PKI 提供接口的 Web 服务，为 Web 服务安全体系中的所有对象提供了可信的安全基础环境。

习　题

一、选择题

1. 目前 Web 服务安全的关键技术有 WS-Security 规范、XML 签名规范、XML 加密规范以及下列哪一项？（　　）

A. SAML　　B. SOAP

C. XKMS　　D. OASIS

2. Web 服务架构的 3 个基本操作不包括下列哪一项？（　　）

A. 发布（publish）　B. 绑定（bind）

C. 请求（request）　D. 查找（find）

二、问答题

1. 简述电子商务安全策略及对策。

2. 简述数据库安全技术的概念及安全体系。

3. 思考如何实现 Web 安全策略。

课后实践与思考

电子商务安全技术实例

（1）登录中国数字认证网 www.ca365.com，申请一个免费的个人数字证书并安装在计算机上。

- 下载根证书并安装。
- 申请个人数字证书并安装。
- 查看所安装的数字证书包含的内容。

（2）将申请的个人数字证书导出到一个文件中（同时导出私钥），并重新再次导入并安装。



注意做好备份。

（3）登录 www.myca.cn。

数字证书　在线编码/解码　在线签名/加密　帮助说明　向MYCA捐款

首页　注册EMAIL证书　注册实名证书　获取证书　查找证书　吊销证书　安装根证书　下载根证书

注册EMAIL证书

选择此选项可以为用户注册一个EMAIL数字证书，此证书使用电子邮件的方式认证。

注册实名证书

选择此选项可以为用户注册一个实名认证的数字证书，此证书使用身份证与电子邮件结合的方式认证。

获取证书

如果您已经注册了数字证书，但是还没有获取，请选择该选项。

查找

选择此选项可以查找一个数字证书，这项功能有助于确定一个数字证书是否有效、过期或已经被吊销。您也可以从此选项下载数字证书。

吊销

选择这个选项可以吊销您的数字证书。如果怀疑数字证书受到危害，则应立即将它吊销。这些危害包括私钥丢失或被盗、密钥对被破坏、所有权变更，以及可疑的欺骗行为。

使用MyCA

如果您还没安装MyCA的根证书，请先安装根证书，以保证您正常的使用MyCA的服务。

如果您想使用MyCA为您提供的安全服务，请注册申请一张专属于您的CA证书，MyCA提供的CA证书可以用于客户端验证、安全电子邮件，并且没有使用时间的限制。如你要申请用于其他用途的CA证书，请联系MyCA（info@myca.cn）

关于MyCA

MyCA提供的证书服务是试用、学习性质的CA服务。

我们不保证也不验证CA证书持有者的真实身份，请您自行验证。

我们也不保证MyCA的绝对安全及永久存在，但我们会尽我们之能力为您提供安全、稳定的CA服务。

整个操作过程如下面的图片所示。

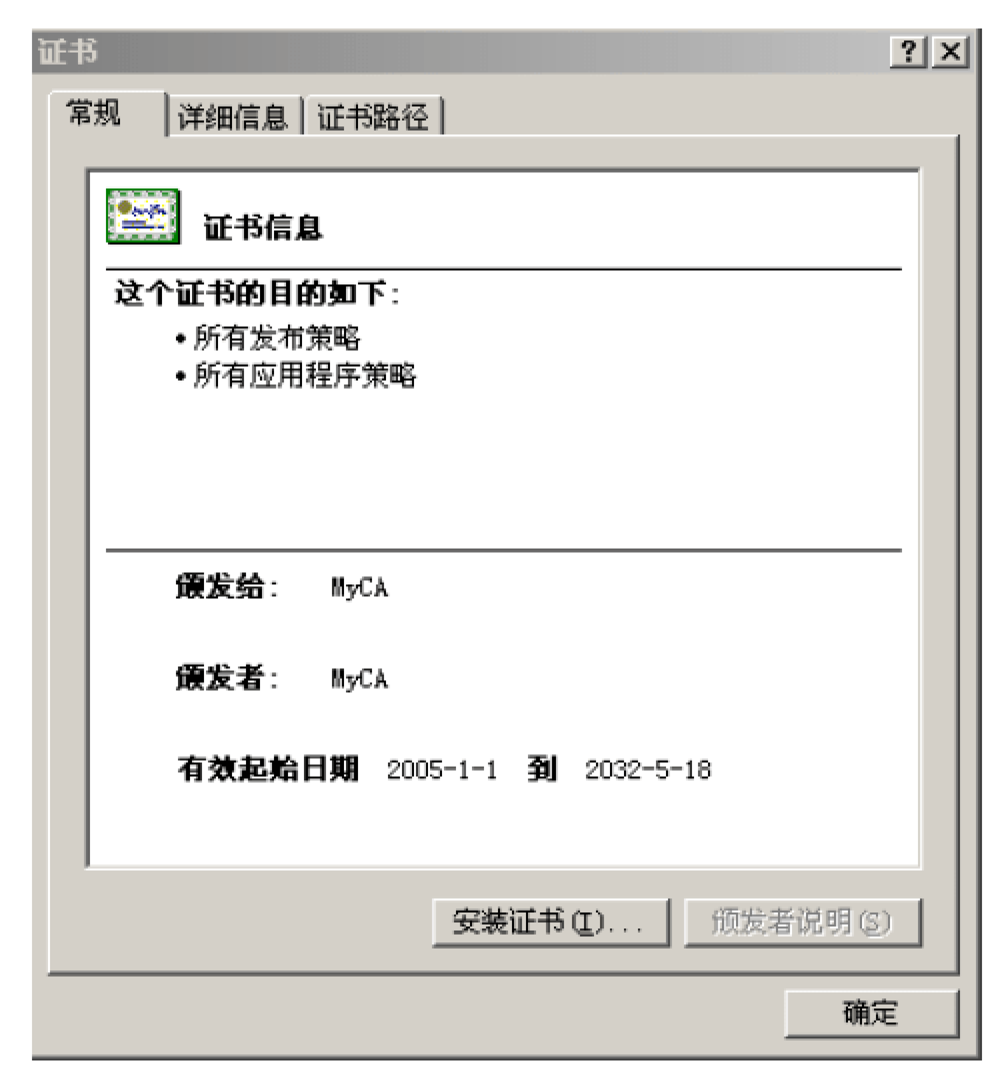
1. 下载根证书并安装

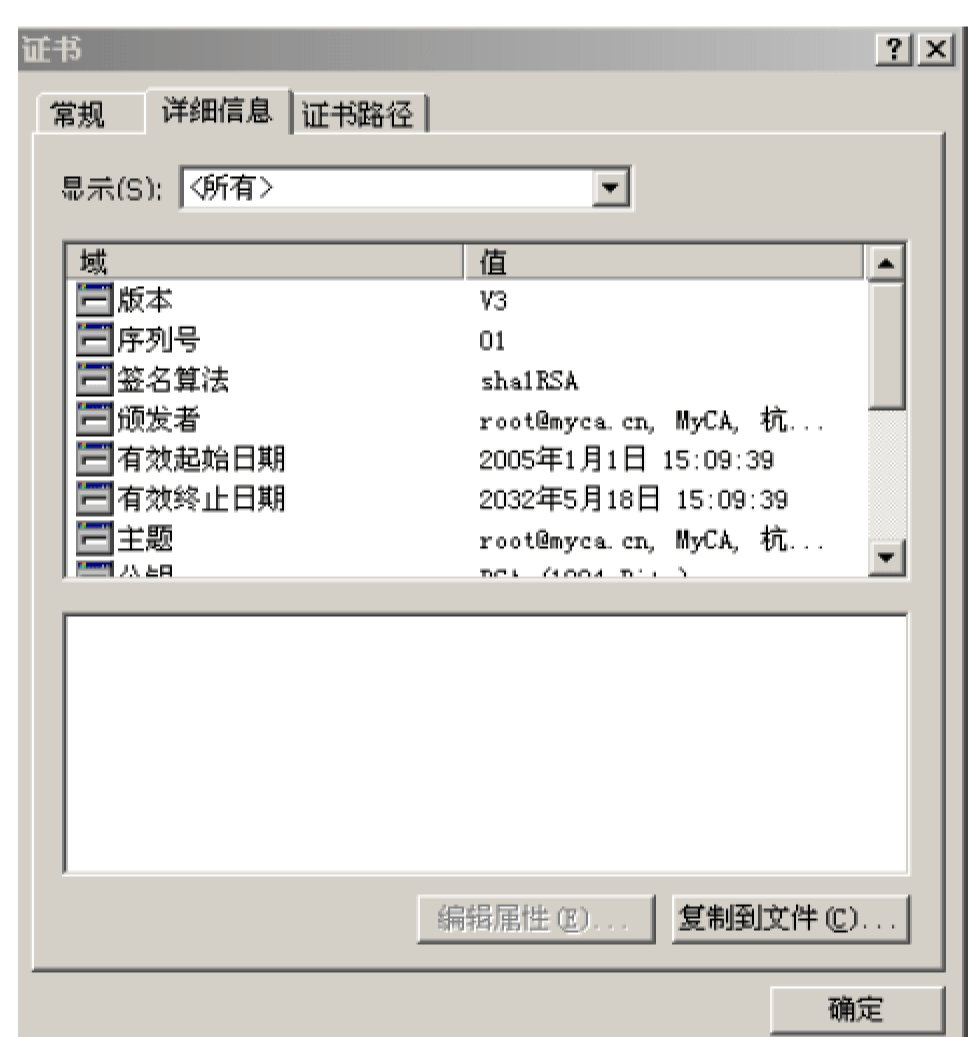
下载MyCA根证书

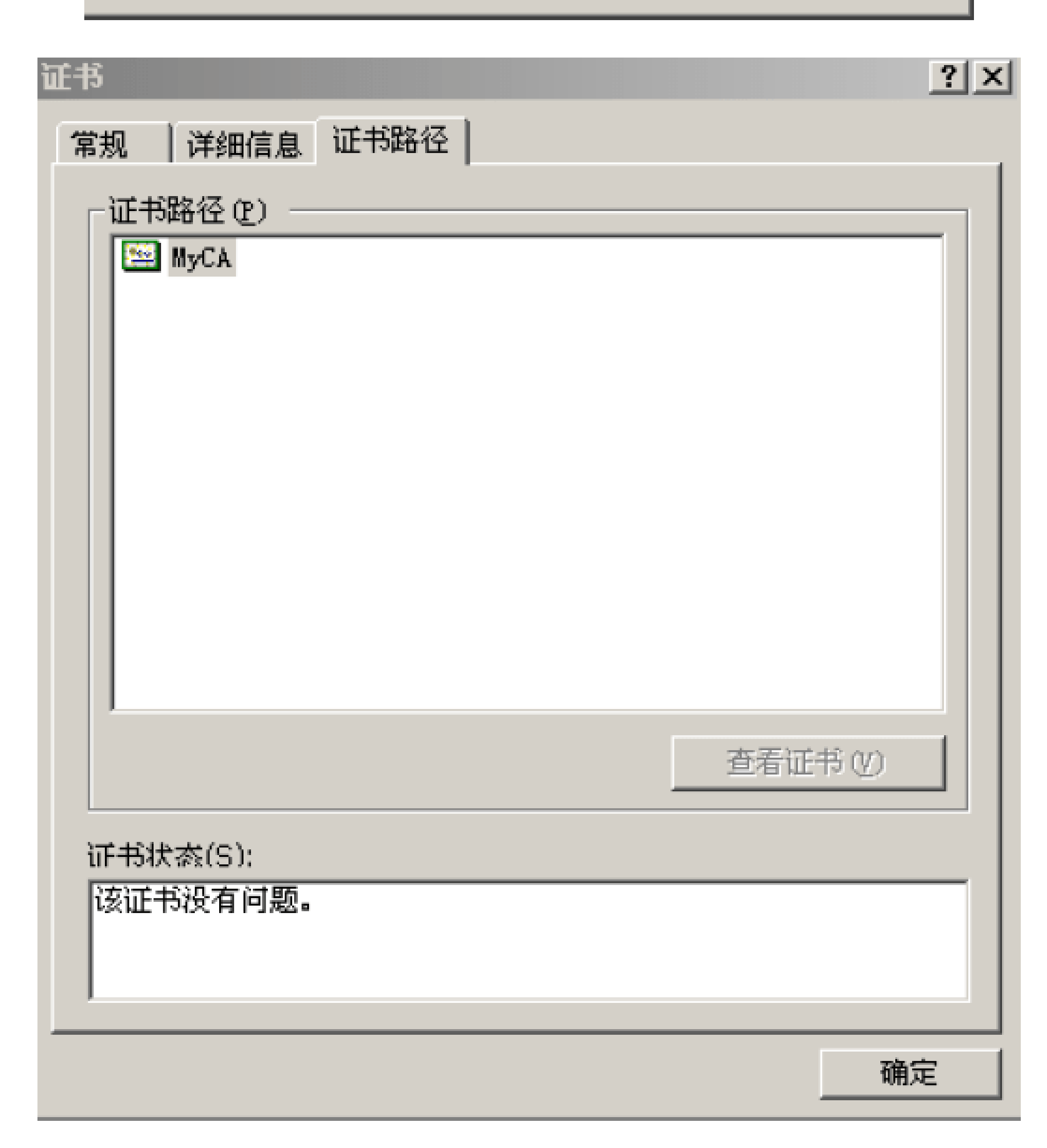
1. 根证书MyCAroot.crt
2. 中间证书一MyCA1.crt
3. 中间证书二MyCA2.crt
4. 中间证书三MyCA3.crt
5. 中间证书四MyCA4.crt
6. 中间证书五MyCA5.crt



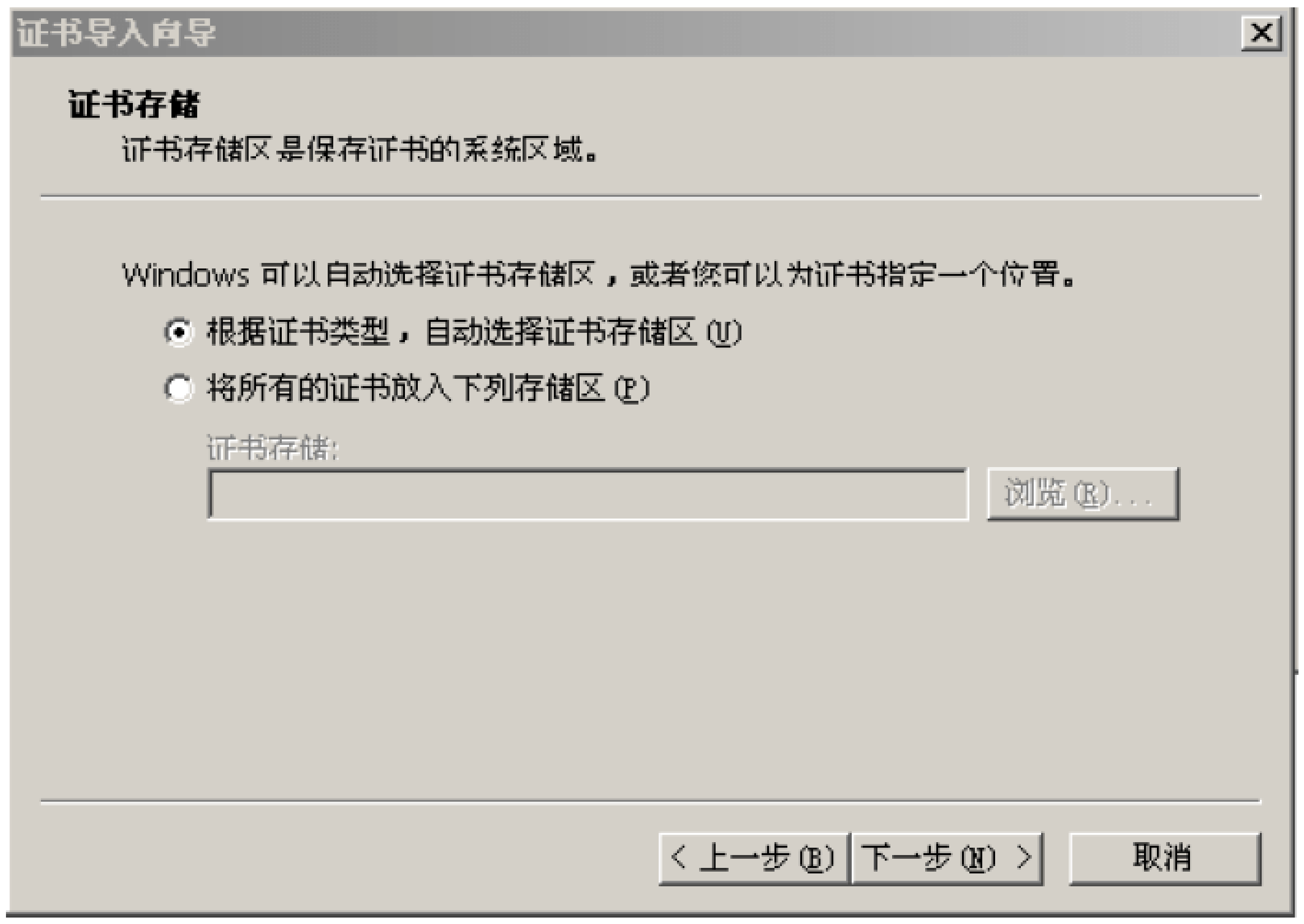
图 17-4　下载 MyCA 根证书


证书
常规
详细信息
证书路径
证书信息
这个证书的目的如下：
• 所有发布策略
• 所有应用程序策略
颁发给：MyCA
颁发者：MyCA
有效起始日期 2005-1-1 到 2032-5-18
安装证书(I)...
颁发者说明(S)
确定


证书
常规
详细信息
证书路径
显示(S): <所有>
域
值
版本
V3
序列号
01
签名算法
sha1RSA
颁发者
root@myca.cn, MyCA, 杭...
有效起始日期
2005年1月1日 15:09:39
有效终止日期
2032年5月18日 15:09:39
主题
root@myca.cn, MyCA, 杭...
编辑属性(E)...
复制到文件(C)...
确定


证书
常规
详细信息
证书路径
证书路径(P)
MyCA
查看证书(V)
证书状态(S):
该证书没有问题。
确定

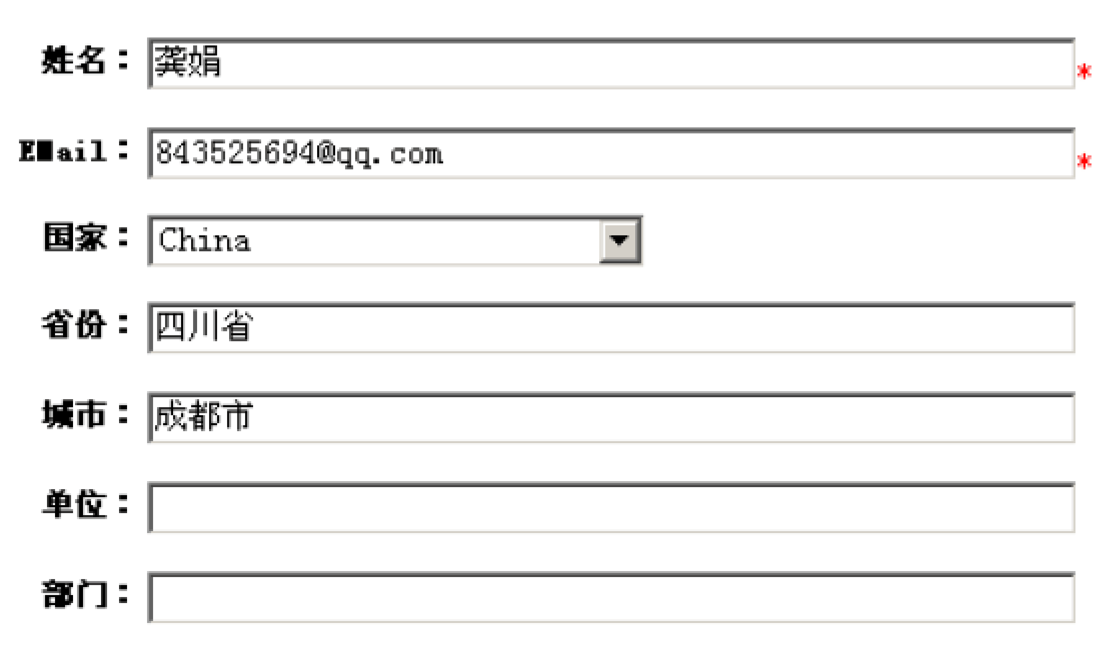

证书导入向导
欢迎使用证书导入向导
这个向导帮助您将证书、证书信任列表和证书吊销列表从磁盘复制到证书存储区。
由证书颁发机构颁发的证书是确认您的身份的文件，它含有用来保护数据或建立安全网络连接的信息。证书存储是保存证书的系统区域。
要继续，请单击"下一步"。
< 上一步(B)
下一步(N) >
取消


证书导入向导
证书存储
证书存储区是保存证书的系统区域。
Windows 可以自动选择证书存储区，或者您可以为证书指定一个位置。
根据证书类型，自动选择证书存储区(U)
将所有的证书放入下列存储区(P)
证书存储:
浏览(R)...
< 上一步(B)
下一步(N) >
取消


证书导入向导
正在完成证书导入向导
您已成功地完成证书导入向导。
您已指定下列设置:
选定的证书存储　被向导自动决定
内容　证书
< 上一步(B)
完成
取消



2. 申请个人数字证书并安装



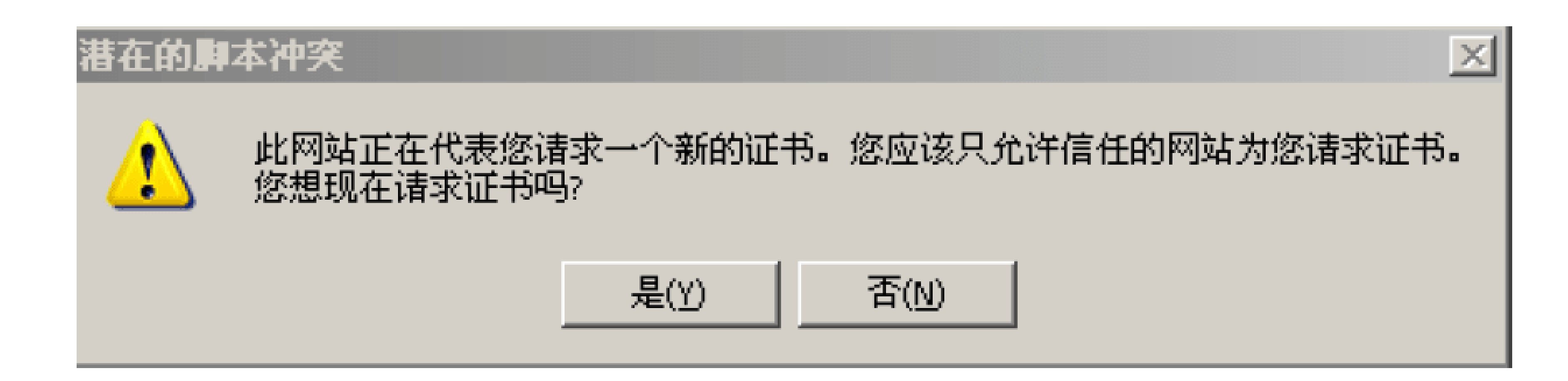


可选项：选择您的加密服务
MS 基本加密提供者提供了512位的密钥，对于大多数人来说，已经足够了， 但是，如果您的浏览器提供了增强选项，您可以使用更高的加密强度。如果您使用智能卡等加密设备，请按照生产者的指导进行操作。

选择您的加密服务：Microsoft Base Cryptographic Provider v1.0

密钥长度：512





发件人：MyCA <free@myca.cn>
时　间：2011年12月2日(星期五) 上午9:07
收件人：843525694@qq.com <843525694@qq.com>

尊敬的 龚娟 先生/女士，
您的管理员已经批准了您的数字证书申请。
要确保其他人不能够获取包含您个人信息的数字证书，
您必须使用唯一的身份识别码（PIN）在十五日内从安全的web站点上取回您的数字证书。
您可以通过下面几个步骤来取回您的数字证书：

步骤 1：访问数字证书获取web页面。
如果您的管理员为获取证书页面定制了一个位置，那您就应该访问您的管理员指定的站点连接。
否则，您可以从下面的站点获取您的证书，

http://www.myca.cn/myca/mspickup.asp

步骤 2：在表格中，输入您的身份识别码：

您的身份识别码是：39ccbd1462899001b4517b26c7447902200118062

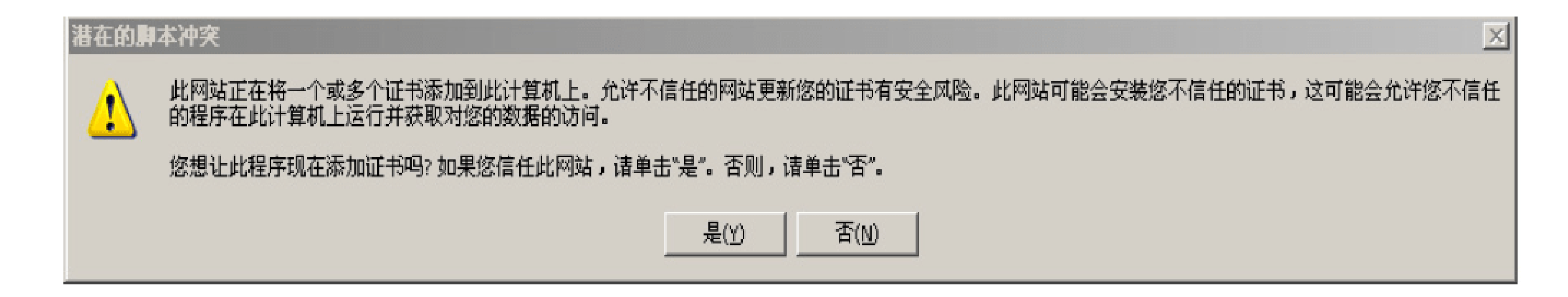
步骤 3：按照页面中的指示来完成您的数字证书安装。

获取证书

重要提示：这一步必须用与注册时相同的计算机(或UKey)来完成。

输入身份识别码（PIN）：
PIN在管理员发给您的确认电子邮件中列出。
39ccbd1462899001b4517b26c7447902200118062

提交



安装证书成功！

返回

3．查看你所安装的数字证书包含的内容

查找结果

本次查询找到了以下符合条件的数字证书。

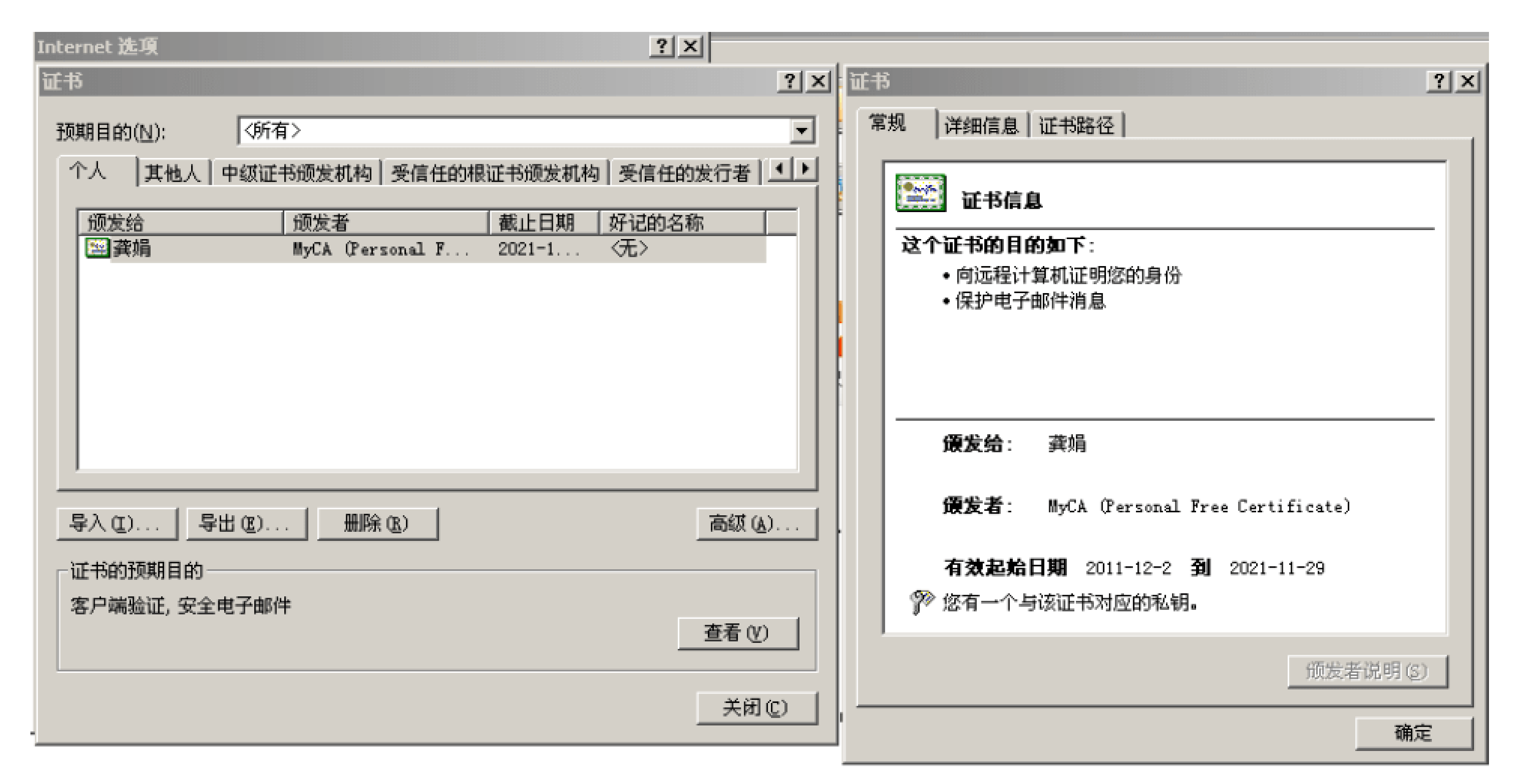
龚娟(有效)

843525694@qq.com

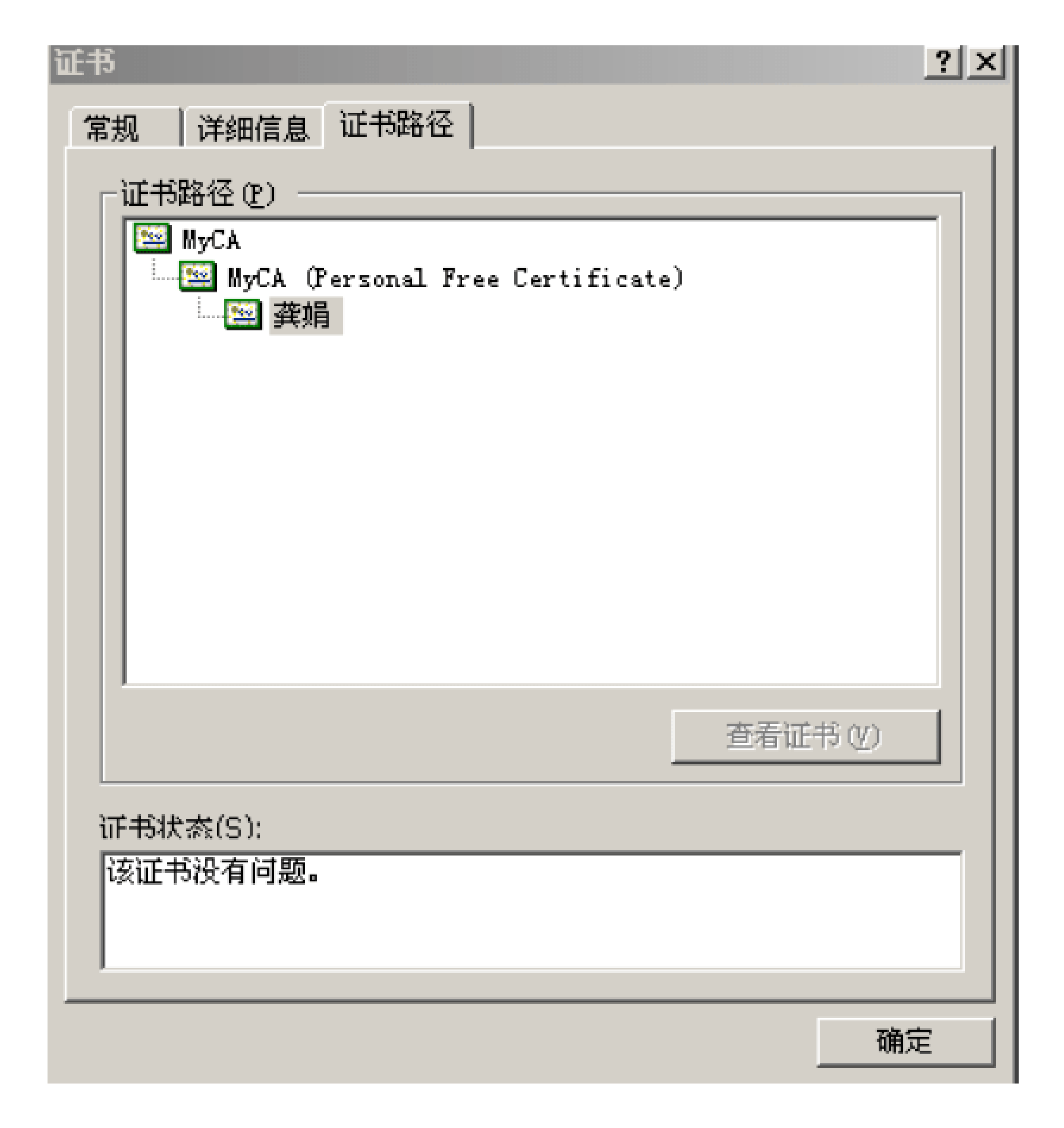
MyCA 个人免费证书

有效期从 2011-12-2 9:07:27 至 2021-11-29 9:07:27

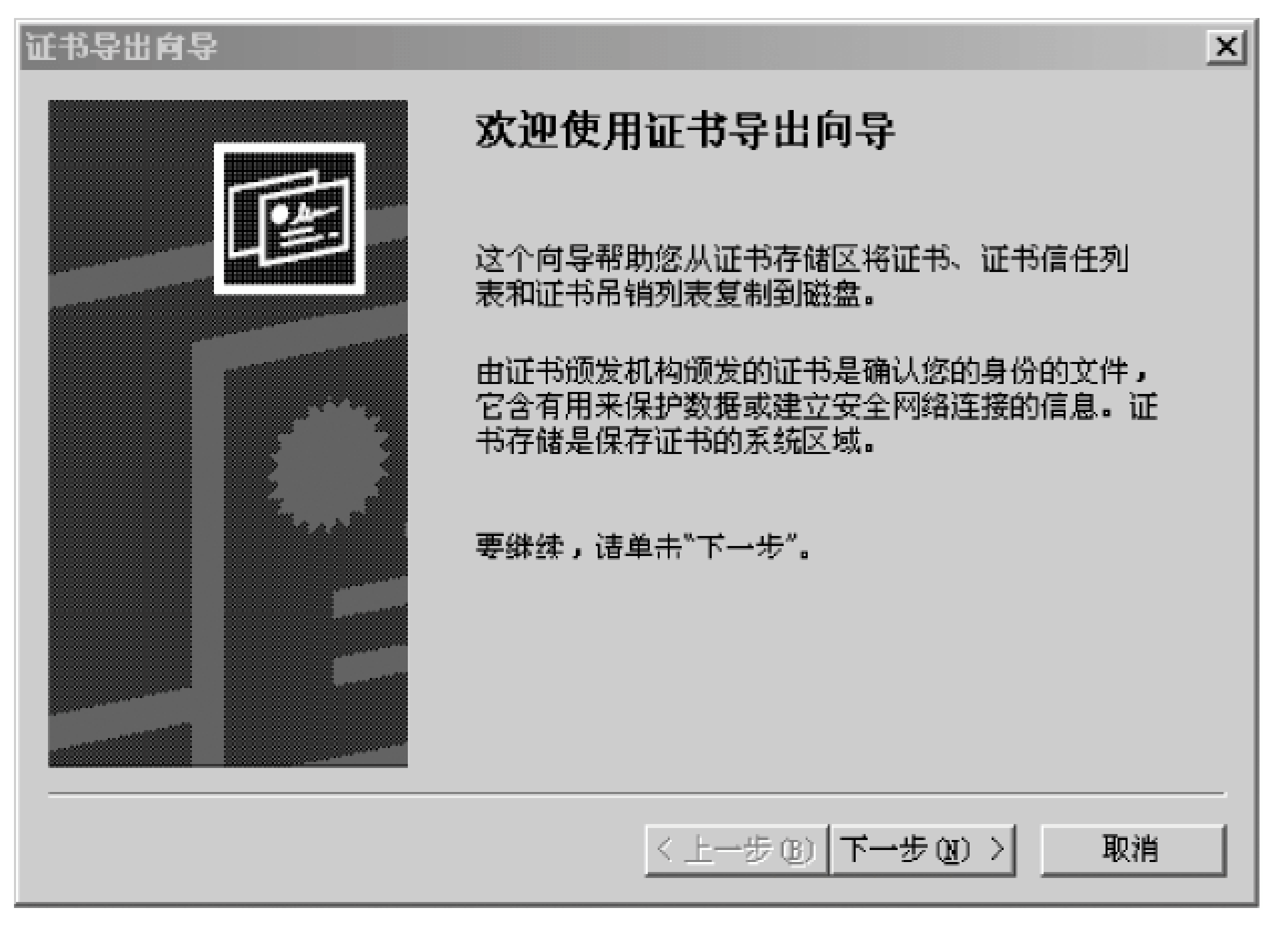
单击“工具”→“Internet 选项”命令，单击安装的证书，单击“导出”按钮。

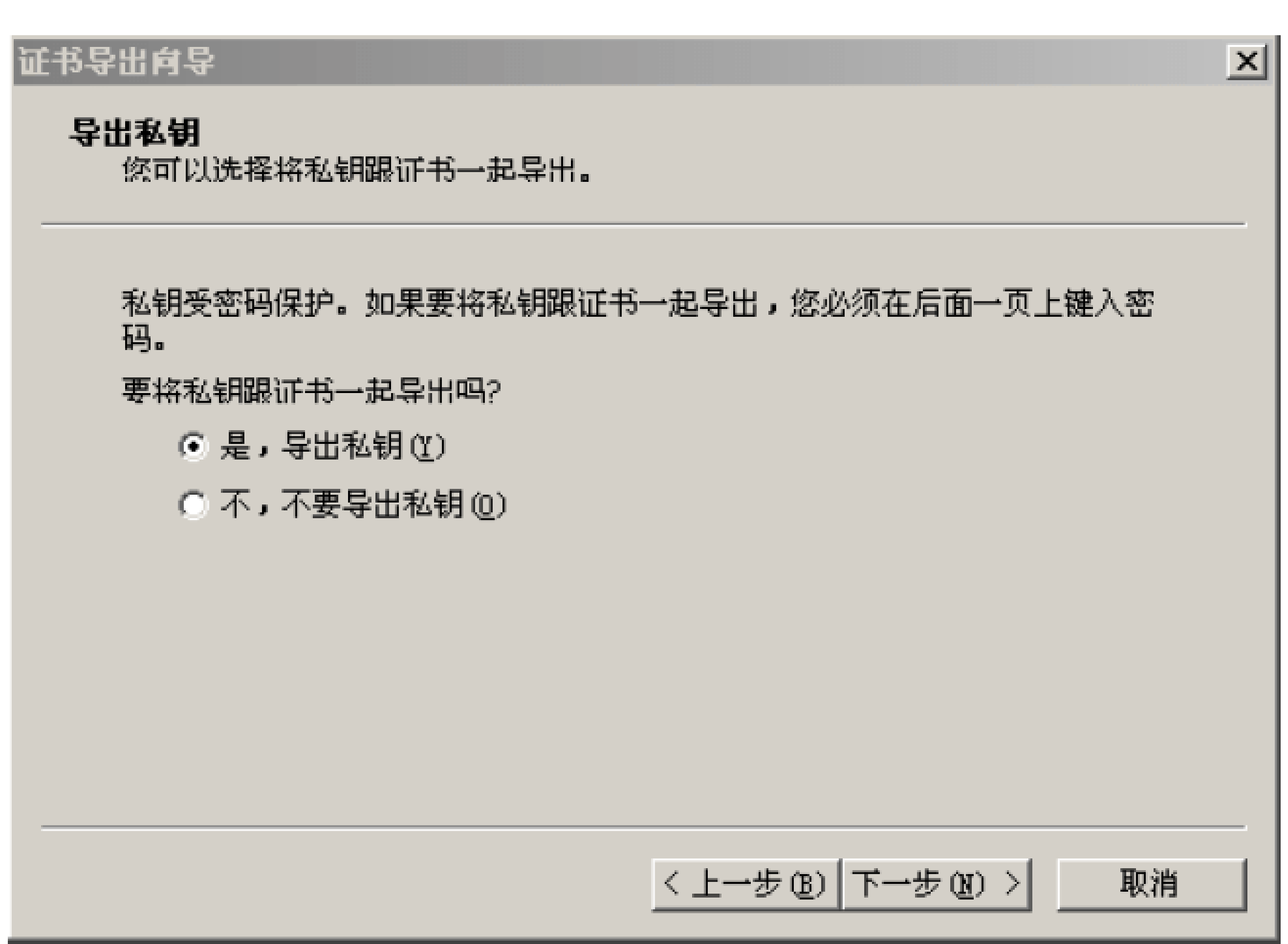


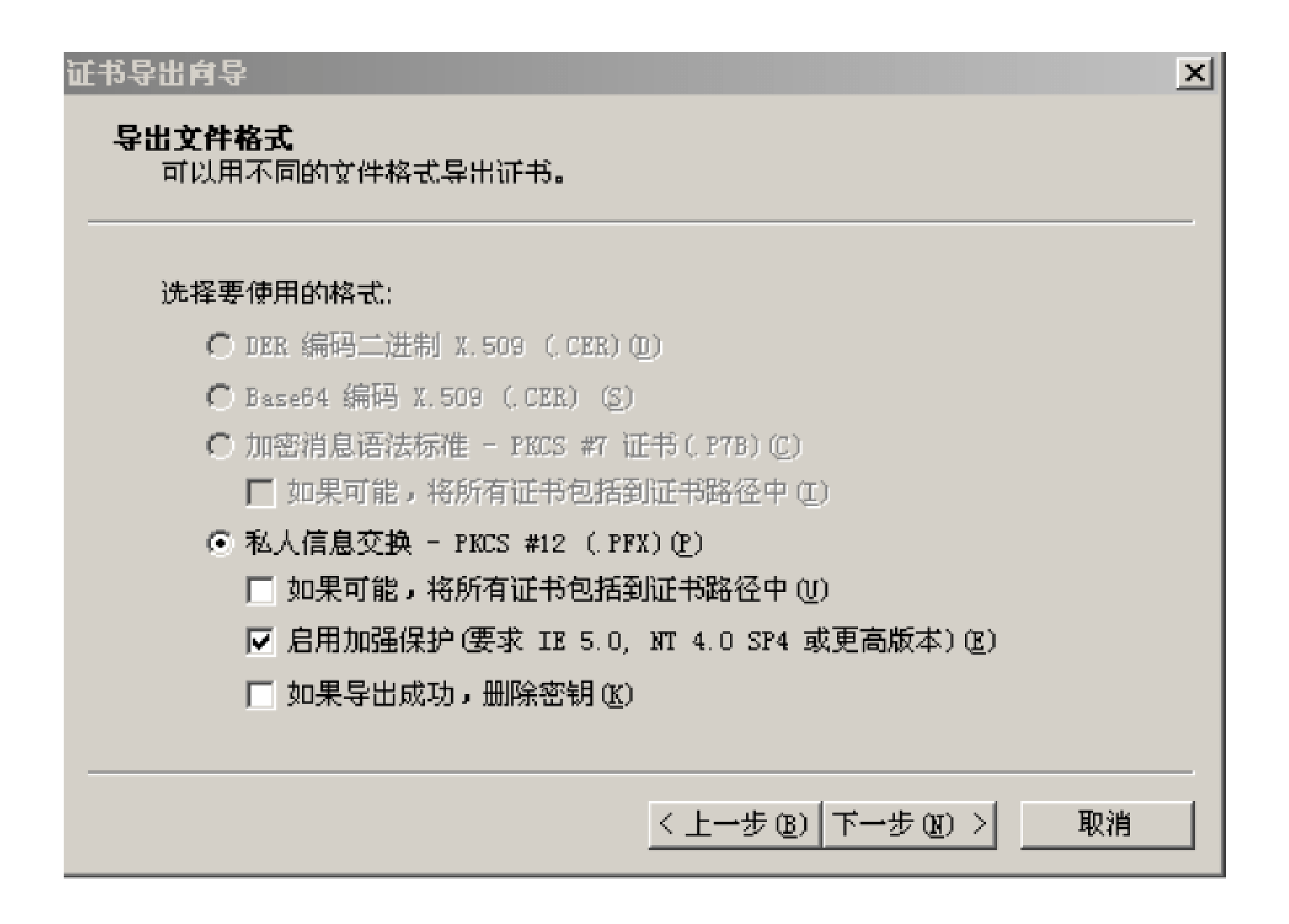




4．将申请的个人数字证书导出到一个文件中（同时导出私钥）







证书导出向导

密码

要保证安全，您必须用密码保护私钥。

键入并确认密码。

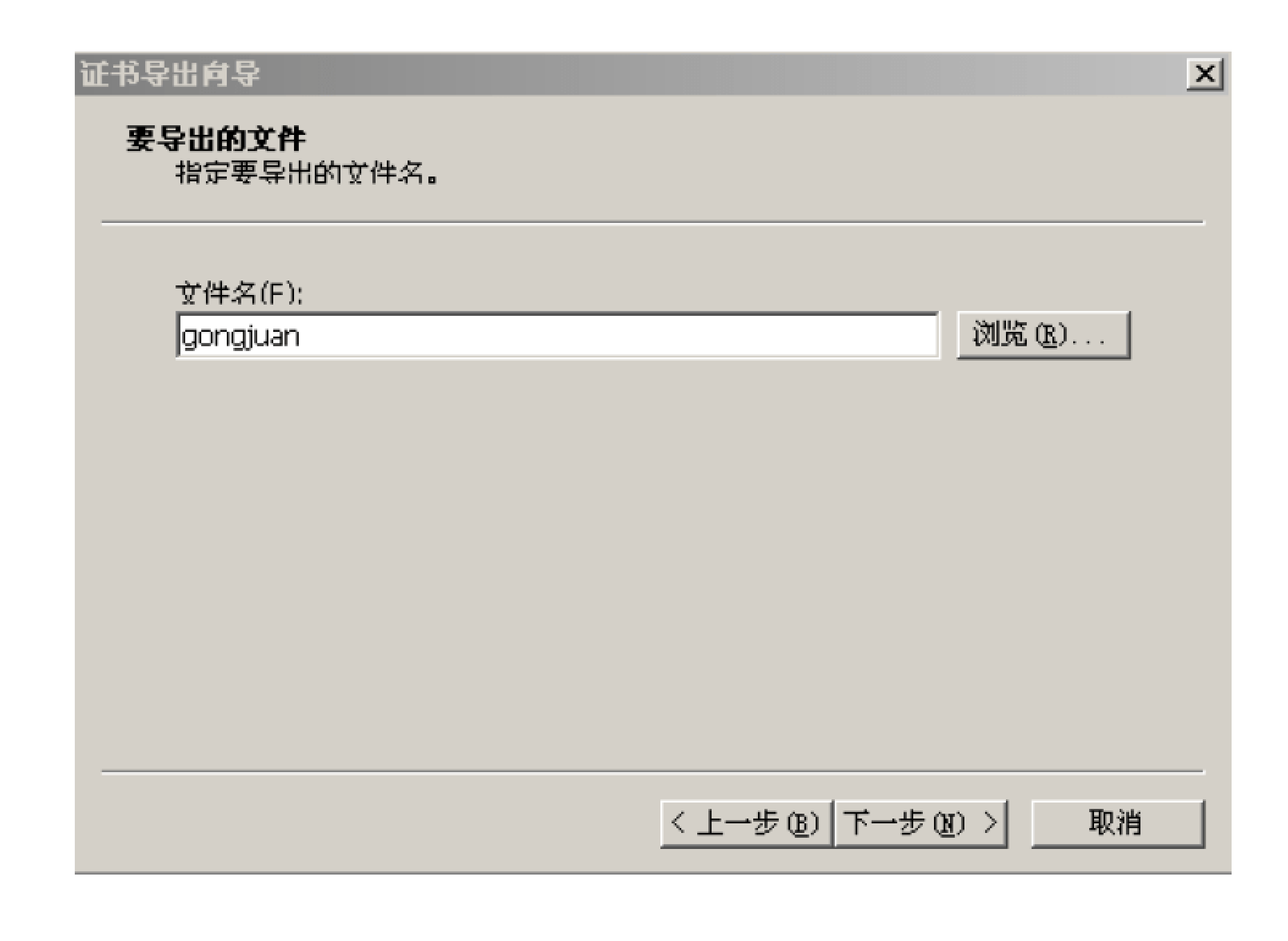
密码(P):

****

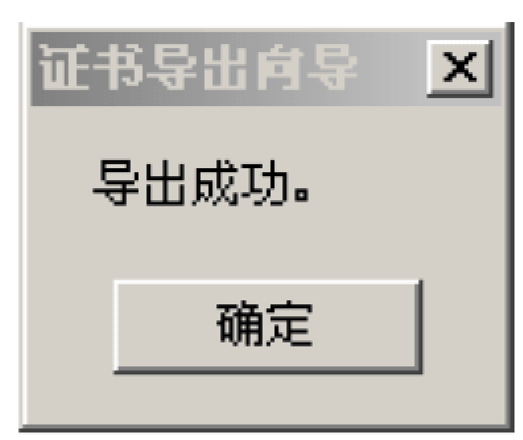
确认密码(C):

****

< 上一步(B) 下一步(N) > 取消



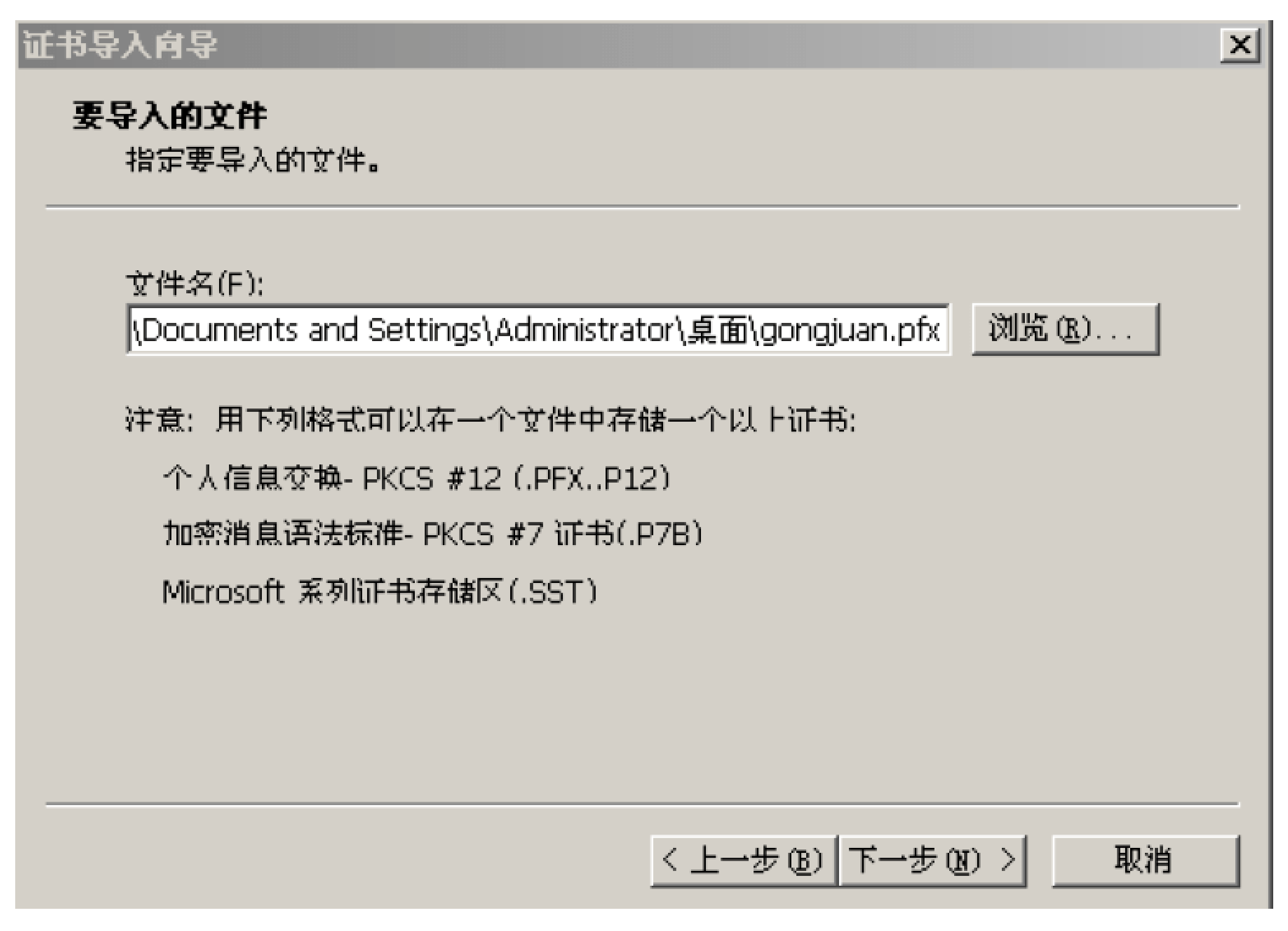


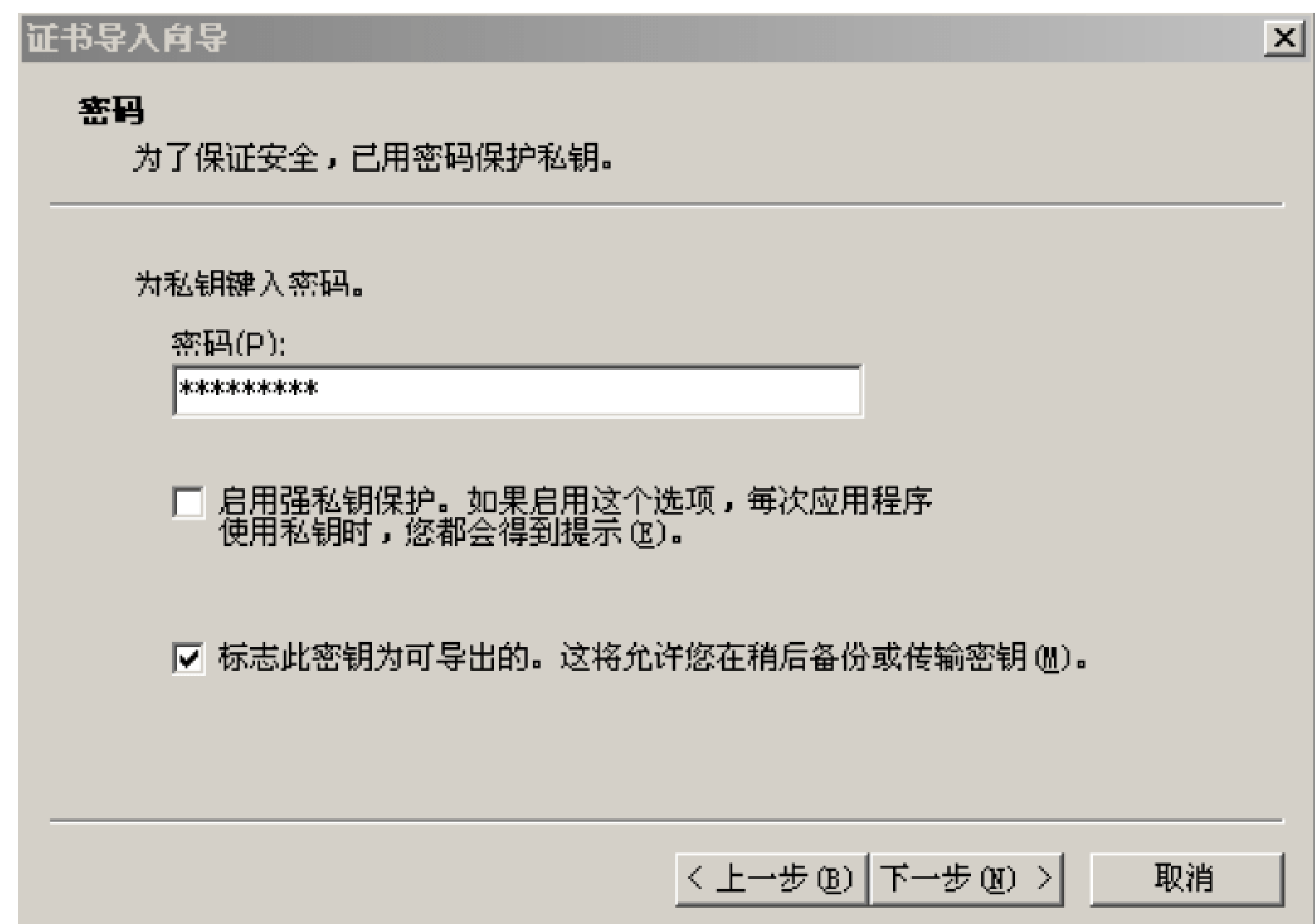


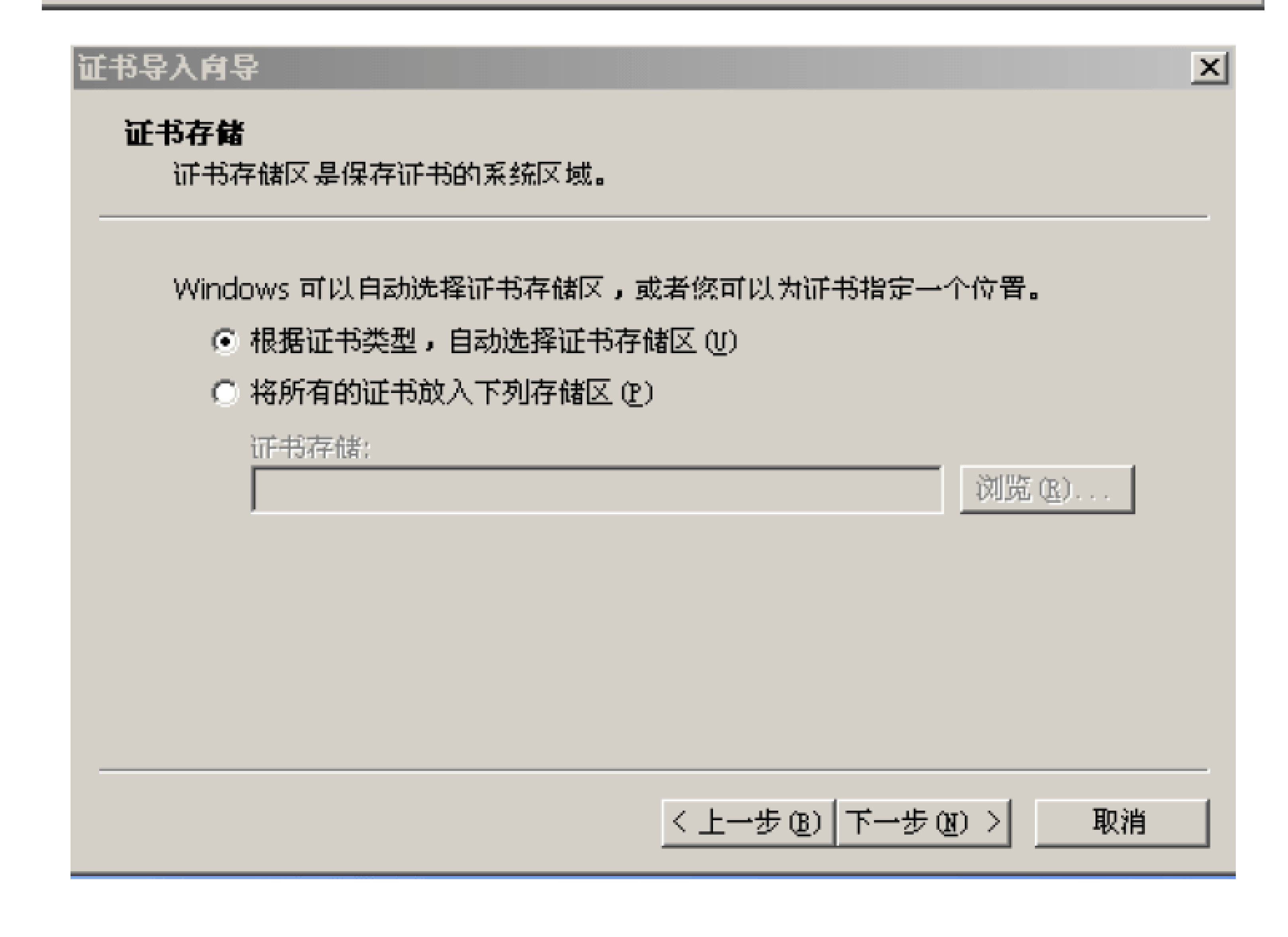


5. 重新再次导入并安装（提示：注意做好备份）




证书导入向导
要导入的文件
指定要导入的文件。
文件名(F):
\Documents and Settings\Administrator\桌面\gongjuan.pfx
浏览(R)...
注意：用下列格式可以在一个文件中存储一个以上证书:
个人信息交换- PKCS #12 (.PFX,.P12)
加密消息语法标准- PKCS #7 证书(.P7B)
Microsoft 系列证书存储区(.SST)
< 上一步(B)
下一步(N) >
取消


证书导入向导
密码
为了保证安全，已用密码保护私钥。
为私钥键入密码。
密码(P):
****
启用强私钥保护。如果启用这个选项，每次应用程序使用私钥时，您都会得到提示(E)。
标志此密钥为可导出的。这将允许您在稍后备份或传输密钥(M)。
< 上一步(B)
下一步(N) >
取消


证书导入向导
证书存储
证书存储区是保存证书的系统区域。
Windows 可以自动选择证书存储区，或者您可以为证书指定一个位置。
根据证书类型，自动选择证书存储区(U)
将所有的证书放入下列存储区(P)
证书存储:
浏览(R)...
< 上一步(B)
下一步(N) >
取消

证书导入向导

正在完成证书导入向导

您已成功地完成证书导入向导。

您已指定下列设置:

选定的证书存储	被向导自动决定
内容	PFX
文件名	C:\Documents and Settings\Admi

< 上一步(B)　完成　取消



第 18 章　信息安全建设标准

本章学习重点：

- 理解最小特权原则的实施与重要性
- 利用深度防御策略来设计一个行之有效的周边防御方法
- 为一个组织或企业编写并执行具体的安全策略
- 利用通用安全管理工具来减轻执行安全策略的繁琐
- 理解通过其他技术措施整合人员与物理安全的意义

信息安全是一项困难而又不被关注的任务——保护组织的数据安全。一般来说，很少会有一个标准去评判这项任务是否是成功的，但如果失败了，结果往往可以显而易见的。设计具体的安全程序是一项复杂的任务，需要平衡用户的合法需求的保密性、完整性和可用性。幸运的是，安全专家们有着可以利用的“财富”，这些财富就是早期安全专家建立的，并在一个知识体系内不断发展的安全实践。这些实践中有很多甚至早于计算机的发展。本章将介绍几个常见的安全实践，这些实践的适用范围小到家庭网站，大到政府系统。而在安全实践之中，防火墙、入侵检测、访问控制等安全措施都不是信息安全“包治百病的灵丹妙药”。这些技术只有适当地用于安全实践中才能成为一个完整的信息安全系统。

18.1　通用安全原则

信息安全不是一个崭新的概念，尽管其在最近数十年内才引起社会的极大关注，但信息安全实践所使用的理念和策略都有着数百年的历史。从古至今，所有类型的组织都要在竞争的环境中保守他们的秘密。将军不希望作战计划被敌人发现；投资专家不希望他们的交易行为的秘密被公众获知；消费品厂商不希望产品的配料或产品制作的诀窍被其竞争对手获知。所有的这一切，组织都会通过利用安全方法来限制相应信息的访问权限。计算机安全产生于 20 世纪 50 年代至 20 世纪 60 年代，并应用在政府部门与军事部门等存储、运行大量敏感信息的系统。

本节将介绍 4 种常见的原则，这 4 种原则已经使用了数百年，前 3 个原则——特权分离原则、最小特权原则、深度防御原则，第 4 种为模糊安全，即通过设置安全区域的方法来保障安全。

18.1.1　通用原则

1．特权分离原则

特权分离原是最久远的安全原则之一，并仍然适用于现在的安全实践中，其思想相

当的简单，不主张单一的人员有足够的权限导致核心事件的发生，该原则不光用于计算机信息安全，还广泛运用于其他的安全领域。

- **空军系统** 没有一个军方官员有权限运行核武器，一般来说释放一个洲际导弹需要两个官员同时扭转其钥匙。两个钥匙的距离要能够保证一个人完成该任务的可能性为零。
- **金融系统** 其手头存放着大量的现金，但不允许任何一个人能够随意进入现金的保险库，当一个人处理现金业务时，还会有其他角色起着监督的作用，如果想要逃避检测，那么必须进行串通，从客观上增加了犯罪的成本。

特权分离在信息安全领域也应用广泛，当设置访问控制或其他安全措施时，安全管理员应该确认在这些安全措施实施不会由于某个单一特权而导致安全需求受到损害。控制的程度取决于所处的行业和处理的信息。任何决定都应该遵循组织的安全策略。例如：建立新账户的权限和给某个账户赋予管理员权限的权限应该分别分配给两个人，这样可以有效地防止一个人建立一个新的账户并同时拥有该账户管理员的权限。

2. 最小特权原则

最小特权原则是特权分离原则的一个扩展，这一原则的内容就是：一个人进行控制或相应的工作职责时，应该只分配最低限度的权限。这是一个显而易见的原则，但同时也是最容易被违反的原则，有两个主要的原因。

- **管理员的疏忽** 通常会无意间分配给用户多余的权限，将用户归类为高权限的组，而事实上其应有的权限小于该权限。
- **权限的变动** 该情况常发生在用户角色发生变化时，在角色变化后却没有及时收回原角色的特权，这样可能在角色频繁变化后可能造成严重的安全问题。为了解决该问题，在任何角色变化后都应该对所有用户的权限进行一次审计。

3. 深度防御原则

在军事方面，军方在很早以前就认识到了建立一个多层次的防御体系来进行防御的重大意义。没有一个国家会将自己的军队沿着边境线排列来抵抗外部的入侵，这样会使敌人有可乘之机，只需集中军事力量攻击某一个区域内，那么就有可能造成整个防线的瘫痪，由此深度保护的概念就可以体现出来了。

信息安全专家将该理念用于信息保护中，在过去数十年里面，深度防御的概念受到了负责设计计算机网络外围保护的安全人员的追捧。这个理念具体包括在访问控制节点建立多层次的安全防护，并在不同的关键点上进行层次间的级联保护，图 18-1 显示了深度防御的一个例子：一个入侵者若想要从外部入侵系统获取敏感信息，首先需要通过边境路由器，然后需要了进一步的渗透进入防火墙和至少一个内部路由器，在渗透同时还需要躲避多个入侵检测系统的检测。

4. 模糊安全

在信息安全早期，安全管理人员常依靠恶意入侵者不知道系统内部所采用的管理安全措施这一事实来保证安全的，这就叫做模糊安全。这种方法在一定程度上是有效的，

尤其是在国防安全的保密系统中。政府部门防止个体获取内部系统信息所采用的安全措施一般是“黑匣子”机制，也就是说不知道内部是如何工作的，只需利用其结果即可。

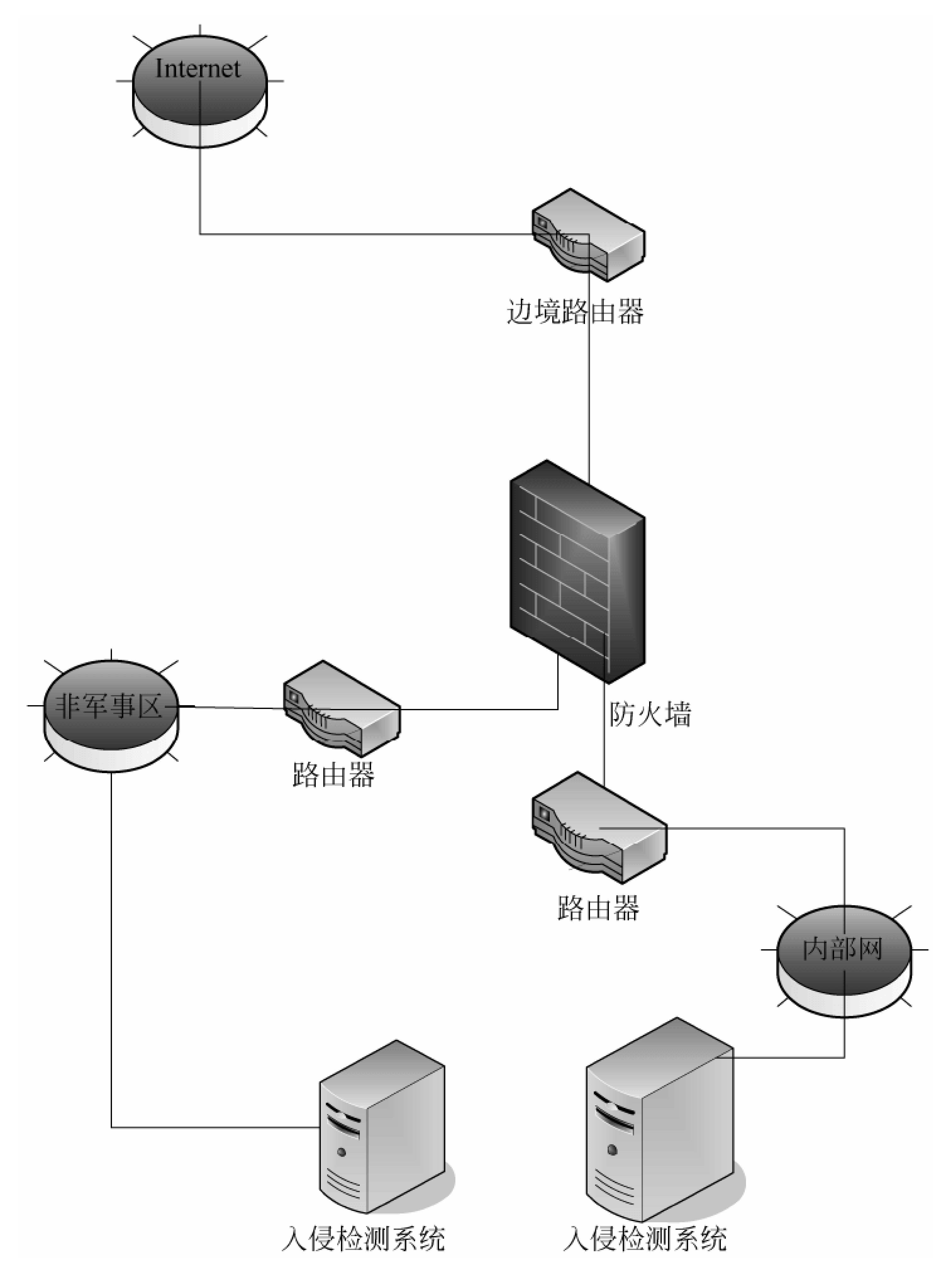


图 18-1　深度防御例子

18.1.2　安全策略

一个有效的安全程序必须明确地定义某个客体所具有的作用，并告知用户可以行使的与之相关的行为。这些都是安全策略通过发展，公布与执行来实现的。这些类型的策略核心功能之一就是告知用户发现与利用安全控制中的漏洞是不被允许的。

每一个企业或组织不管其规模大小都应该起草一份信息安全策略。该文档应该免费为组织内所有用户所使用。但只有一个安全策略的文本是远远不够的，用户还必须进行合适的训练来适应相应的策略，训练往往发生在刚进入公司时或岗位变换时。

1．安全策略种类

安全管理员可以为系统选择数百种不同的安全策略。有着简单基本要求的公司就只

需要一个包含着具体规则和规程的文档来描述企业的安全需求。而一些有着复杂的安全需求的公司可能对安全策略的要求会更高点，包括对每一种突发事件的应急处理和对组织内每一个角色如管理员、经理、用户等有相应的不同的行为要求。

下面将介绍几种常见的安全策略。

（1）可接受使用策略

基本上每一个组织都有可接受使用策略。这些策略阐明了组织内可以允许使用的信息资源。不同的角色有着不同的需求，如经理、雇员、合作伙伴、顾客。

可接受使用策略真正具有挑战的一点是做到让策略能够有效地限制用户权限范围内的行为，同时还要求可以应付不可预知的行为。例如，P2P 网络的发展就要求了很多公司必须修改他们的安全策略，但有些公司就没有修改的必要，因为他们的策略中已经提及了“用户不能将文件分享到组织网络之外”，该策略很有效地囊括了很多无法预料的情况。

作为可接受使用策略，必须能够解决以下问题。

- ❑ 哪些类型的行为是可以被接受的。
- ❑ 哪些类型的行为是不可能被接受的。
- ❑ 如果策略的某方面描述不够细致，那么用户该怎么办。
- ❑ 违反了可接受使用策略后，系统应该采取哪些措施。
- ❑ 违反了可接受使用策略，应当受到什么处罚。

这些问题的答案应该与组织的具体文化相对应，有些企业就允许雇员在工作时间使用网络，甚至提供了一些与工作不相关的功能，而有些企业就完全不允许雇员在工作时间内做任何与工作无关的事情。

（2）备份策略

一提到信息安全，很多人首先就会想到保密性，但完整性和可用性同样不可忽视。所以备份策略的重要性不言而喻。所谓备份策略就是为了应付组织内被保护的数据丢失或损坏的情况。

备份策略应该有以下几方面的内容。

- ❑ 哪些数据需要备份？
- ❑ 如何对这些数据进行备份？
- ❑ 数据应当备份在什么地方？
- ❑ 哪些人有权限接触这些备份介质？
- ❑ 备份数据应当保留多长时间？

（3）保密策略

保密策略描述的是组织内应当受保护的敏感信息所采取的措施，保密策略至少应当有以下内容。

- ❑ 哪些数据是需要保密的？
- ❑ 应该如何处理机密信息？
- ❑ 如果机密信息被非授权泄露了，需要采取哪些应急措施。

很多企业都会要求新员工在进入企业之前签署保密协定，值得注意的是，企业还需要员工即使在他们离开组织后仍然要保护信息的私密性，如果他们违反相关政策，该组

织保留现任和前任雇员的法律诉讼权。

（4）数据管理策略

数据信息是现代企业的命脉，企业就需要有些详细的策略进行数据的管理。数据管理策略包含以下几方面因素。

- **数据类型** 数据管理策略需要提供不同类型数据的保护。因为不同类型的数据有着不同的管理要求。
- **最短保管时间** 策略需要指出每种类型的数据管理的最短时间，该信息的主要目的就是根据法律法规，业务需求或其他要求来确保重要数据的保管时间，例如根据国际税收服务规定，财政与税收相关的信息应当保管至少 7 年。
- **最长保管时间** 策略需要指出每种类型的数据管理的最长时间。这一般用于保管有关私人隐私，组织隐私中的一些数据，根据法律法规的要求需要在一定时间内删除。

以上可以看出，数据管理策略的总体目标就是确保在对商业数据的管理和存储时，所有操作都是在法律法规的允许范围之内的。

（5）无线设备策略

无线设备，例如移动电话、私人商务工具、便携式电脑和其他快速发展的移动设备。随着通信技术的发展，为应付工作地点的无线设备增加的情况，企业组织内需要执行内部范围的无线设备策略。通常无线设备是很难受控制的，并能给系统造成很多的安全威胁。

无线设备策略主要包含以下几方面内容。

- 组织购买的设备类型。
- 员工自带的私人设备类型。
- 允许私人设备行使的行为。

无线设备能够给组织造成很大程度的安全威胁，所以在制订该策略时应当小心谨慎，并能够有力地执行下去。

2. 策略执行

负责安全策略的挑战之一就是策略的执行。政策的生命周期包括政策制订、验收、培训、执法和维护等几部分，有些过程可以一次性地完成，但也有很多过程是随着组织的发展而不断地适应变化的。

（1）政策制订

信息安全策略的制订一般通过团队方式处理。只有这样才能最大程度的包括不同功能因素。通常来讲，这样的一个团队应该包括以下几类人：IT 专家、营业单位代表、物理安全代表、人力资源代表、金融代表、执行管理层代表。

只有在这样的合适的小组组建完成后，才可以开始制定组织的安全策略，一般来说，制订的第一步就是列举出该安全策略需要完成的一系列的商业目标，然后针对每一个目标单独制订出响应的安全策略，下一步是将这些安全策略传播到小组每一个成员手上，进行讨论，修改，最后在大家都同意的情况下，将修改好的安全策略内容汇总在一起，形成一个完整的安全策略。

（2）建立共识

当小组成员对安全策略达成了一定的共识后，那么就应该在组织内部继续传播共识，向组织内的主要管理人员解释安全策略背后的原因。当然在建立组织范围内的共识这一过程中，策略制订小组的高层管理人员代表将发挥重要作用。因为将安全策略进行推广的最有效的方式之一就是由一名高层管理人员将安全策略通过电子邮件或书信的方式进行通告。如果这一步实施顺利，那么未来的执行一步就会容易很多，相反如果组织内部的共识建立失败了，那么该策略就很容易被某些组织内部的人员所忽略。

（3）人员培训

人员培训，即向所有被策略影响的员工提供有效的教育与训练。值得注意的是这一过程不是推广，而是向用户提供有关政策执行方面的细节。

一个完整的培训过程有两个不同的阶段：初始阶段和复习阶段。

- **初始阶段** 该阶段是面向所有新员工或者准员工，该培训目的是提供个人安全责任方面完整的概述。如果无法对新进雇员进入组织的第一天进行培训的话，那么培训应该至少在员工第一次使用计算机系统前进行。关于培训的方式，可以一次性的进行一天或多天的会议来达到强化安全责任的目的，也可以进行一次简短的会议，只是强调一些目标和安全责任的重要性，随后根据个人的需要订购相关的录像带与其他的媒体。

- **复习阶段** 该阶段是面向长期聘用后的员工的。一般在员工的聘期内周期性的进行。复习阶段的培训时间应该相对短点，其有两个目的，第一个就是让员工回顾一下自己在组织中所承担的安全责任，第二个就是一个机会向员工们解释一些由于新近技术的发展导致组织安全策略的修改。复习阶段的培训的范围与方式取决于组织的具体情况。例如：如果组织内经常进行涵盖各种主题的训练会议，那么该培训就可以安排在某一个会议之中进行。

另外需要注意的是，组织提供的安全培训应针对不同的角色定制具体的培训内容。确保培训的内容与个人的工作职责和受教育程度相符合。

（4）策略执行

为了使安全策略有效，其必须在组织范围内贯彻执行。策略本身就应该包含强制执行规定，明确阐明违反政策行为和应遵循的程序时候所负的责任。一个不被执行的策略不管有多么的完善都是没有意义的。

（5）策略维护

可以这么说，安全策略是一个动态的文档。当制订策略时，策略小组的成员致力于策略足够的完善，以至于能够囊括所有未预见的情况，但这是不太现实的，因为每一天都会有改变发生。策略需要通过一系列的标准化过程对自身进行修改。为了确保安全策略能够符合组织当前的计算环境，组织通常会要求安全策略小组成员对安全策略进行定期的审查。

18.1.3 安全管理工具

和其他领域的专家一样，安全从业者也有一系列标准化的工具用于日常工作，有些

是技术类的，例如防火墙、入侵检测系统、漏洞扫描器等，还有一部分是管理工具，常用于安全策略的修改和维护，如下面将要介绍的安全校验表和安全矩阵。

1. 安全校验表

校验表在信息技术中属于最为流行的管理工具，通用于大型或小型组织。安全专家使用校验表用于截然不同的目的。①安全专家应该审阅组织当前存在的安全清单，确保概述的程序与组织内的信息安全策略一致。通过对校验表中的项目进行增加、删除、修改，从而快速有效地修正用户的日常行为。②安全从业者可能希望建立自己安全校验表用于具体的安全目的。这些检验表可以是完全重新设计或者通过借鉴别人的经验设计的。

2. 安全矩阵

安全矩阵是一个用于安全策略制定和具体执行的工具。表 18-1 即为一个简单安全矩阵，表格的行为信息安全的 3 种属性，列为影响程度。系统管理员在为系统制定安全进程时，应该针对每种情况完成相应的安全矩阵。该矩阵可用来帮助指导安全资源的有效利用。

表 18-1 一个简单的安全矩阵

	保密性	完整性	可用性
非常重要		X	X
一般重要			
次重要	X		

18.1.4 物理安全

另外一个容易被忽略的安全就是物理安全，公司在技术方面投入了大量的人力物力，防止黑客通过网络非法进入系统获取资源。但同时也应该确保安全守卫在岗以防止任何人能够简单地到达服务所在的位置。除此之外，物理安全还包括防止火灾、水灾等自然灾害对计算机造成的物理损害。

本节将介绍两种面向主要的信息安全专家的物理安全解决方案：边界防护和电子实体。

1. 边界防护/访问控制

边界防护，与防火墙放在网络边界来保护网络的原理一样，可以建立合适的防御来防止物理设施受到入侵。防御的方式有以下几种：栅栏、运动检测器、巡逻。

防御的等级很大程度上取决于该设施的用途和位置。军方的设施就需要士兵武装巡逻，而校区的服务器就不需要这么大张旗鼓了。

信息安全领域的深度防御原则也可同时用于物理安全领域。对于核心资产，需要对其进行一层又一层的保护。例如：一个要保护的设施，首先用倒刺铁丝围栏围起来，只留一个出入口，要想找到出入口需要通过一个岗哨，同时要出示自己的身份，最后在存

放该设施的房门，需要同时通过指纹和视网膜扫描后才能通过。这样一个深度防御的例子可以形象地表现出，防御层次越高，就越可以提升物理设施的安全性。

2. 电子实体保护

每一个电子设备都会在运行过程中无意识地发出电磁辐射。对于终端用户来说，这些不是很重要，因为没有研究表明这些辐射能够伤害人体，然而，这些辐射却可以为信息安全造成很大的安全威胁，威胁的程度取决于这些辐射所承载的数据内容。事实上，在数百米远的地方可以通过对这些辐射的利用而重新恢复出其承载的内容。

18.1.5 人员安全

不管采取了什么样的安全控制，人员将永远是任何系统中的最薄弱环节，因此在整体的信息安全方案中包含人员安全是至关重要的。主要可采取以下几种措施。

（1）在为员工提供就业时，应该首先进行背景调查。这些调查应包括犯罪记录、信用记录、驾驶记录、教育证明和相关评估。不同的企业关注的方向也不一样，总的来说，可以在一个基础上进行背景调查。

（2）对员工的行为进行监控。具体包括监控网络流量来识别不适当的行为，在敏感位置设置摄像机，记录电话对话。

（3）强制假期。强制假期有两个目的，第一是给员工提供一个休息的机会；第二是可以乘此机会发现原来员工可能隐藏的违规行为。

（4）尽可能的提供给要离开公司的员工一个友好的环境。只有这样他才可能在离开以后执行保密协定。

18.2 安全标准

随着计算机技术的飞速发展，众多标准化组织制定了大量与计算机安全相关的标准。这些安全标准事实上已经成为了各大产商生产计算机产品时所遵循的标准。图 18-2 简单描绘了信息技术安全评估标准的历史和发展。下面列出了一些当今计算机工业界最常用的计算机安全标准及其发展历史。

18.2.1 TCSEC

TCSEC（Trusted Computer System Evaluation Criteria，可信计算机安全评价标准）标准是计算机系统安全评估的第一个正式标准，也称为橘皮书，具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准，后来延至民用领域。TCSEC 将计算机系统的安全划分为 4 个等级、7 个级别。

对 4 个安全等级说明如下。

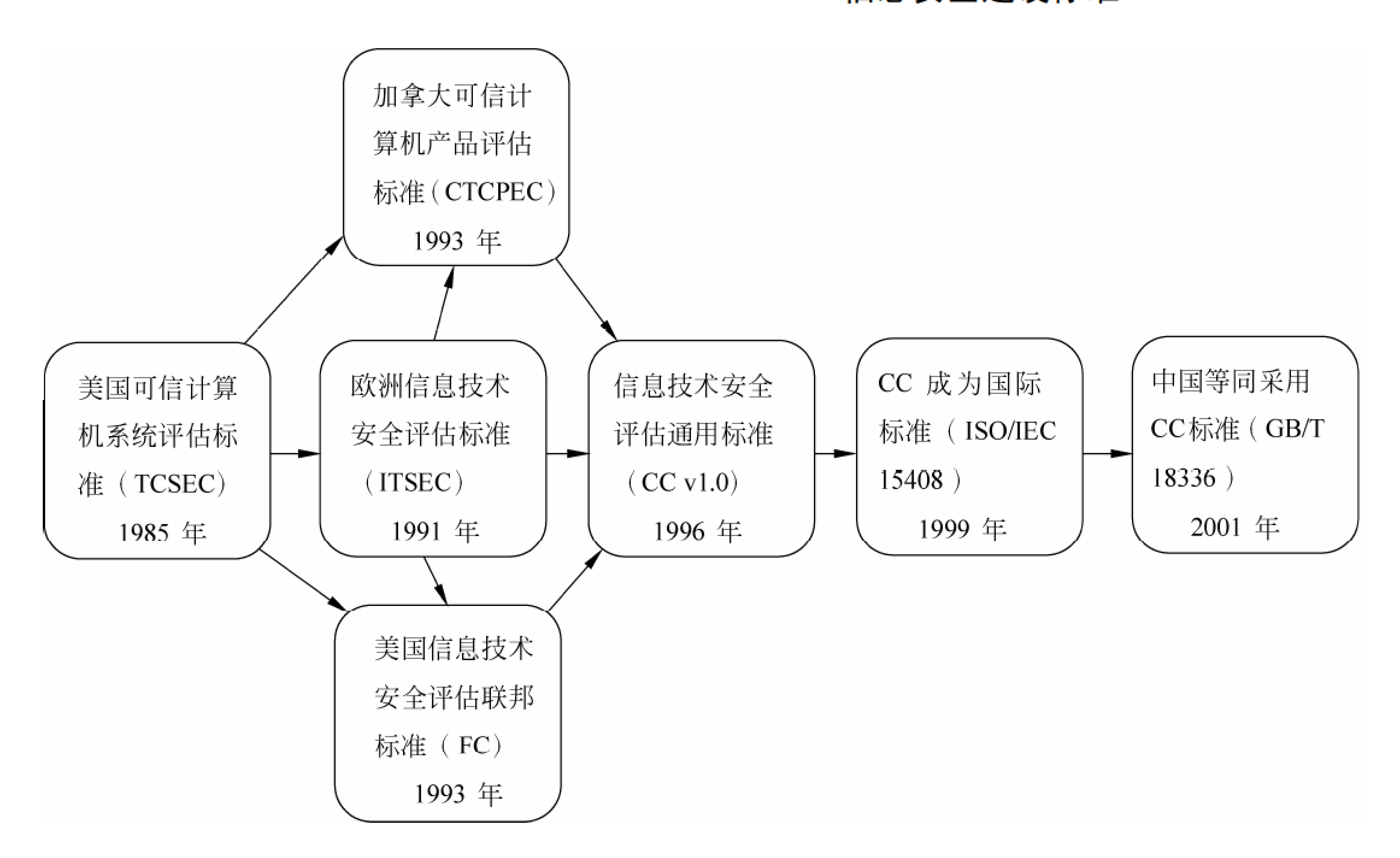


图 18-2　信息技术安全评估标准的历史和发展

1. D 类安全等级

D 类安全等级只包括 D1 一个级别。D1 的安全等级最低。D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

2. C 类安全等级

该类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。C1 系统的可信任运算基础体制（Trusted Computing Base，TCB）通过将用户和数据分开来达到安全的目的。在 C1 系统中，所有的用户以同样的灵敏度来处理数据，即用户认为 C1 系统中的所有文档都具有相同的机密性。C2 系统比 C1 系统加强了可调的审慎控制。在连接到网络上时，C2 系统的用户分别对各自的行为负责。C2 系统通过登录过程、安全事件和资源隔离来增强这种控制。C2 系统具有 C1 系统中所有的安全性特征。

3. B 类安全等级

B 类安全等级可分为 B1、B2 和 B3 共 3 类。B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B1 系统满足下列要求：系统对网络控制下的每个对象都进行灵敏度标记；系统使用灵敏度标记作为所有强迫访问控制的基础；系统在把导入的、非标记的对象放入系统前标记它们；灵敏度标记必须准确地表示其所联系的对象的安全级别；当系统管理员创建系统或者增加新的通信通道或 I/O 设备时，管理员必须指定每个通信通道和 I/O 设备是单级还是多级，并且管理员只能手工改变指定；单级设备并不保持传输信息的灵敏度级别；所有直接面向

用户位置的输出（无论是虚拟的还是物理的）都必须产生标记来指示关于输出对象的灵敏度；系统必须使用用户的口令或证明来决定用户的安全访问级别；系统必须通过审计来记录未授权访问的企图。

B2 系统必须满足 B1 系统的所有要求。另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B2 系统必须满足下列要求：系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变；只有用户能够在可信任通信路径中进行初始化通信；可信任运算基础体制能够支持独立的操作者和管理员。

B3 系统必须符合 B2 系统的所有安全需求。B3 系统具有很强的监视委托管理访问能力和抗干扰能力。B3 系统必须设有安全管理员。B3 系统应满足以下要求：除了控制对个别对象的访问外，B3 必须产生一个可读的安全列表；每个被命名的对象提供对该对象没有访问权的用户列表说明；B3 系统在进行任何操作前，要求用户进行身份验证；B3 系统验证每个用户，同时还会发送一个取消访问的审计跟踪消息；设计者必须正确区分可信任的通信路径和其他路径；可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪；可信任的运算基础体制支持独立的安全管理。

4. A 类安全等级

A 系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收到一个安全策略的正式模型；所有的安装操作都必须由系统管理员进行；系统管理员进行的每一步安装操作都必须有正式文档。

18.2.2 ITSEC

欧洲的安全评价标准（Information Technology Security Evaluation Criteria，ITSEC）是英国、法国、德国和荷兰制定的 IT 安全评估准则，较美国军方制定的 TCSEC 准则在功能的灵活性和有关的评估技术方面均有很大的进步。

ITSEC 是欧洲多国安全评价方法的综合产物，应用领域为军队、政府和商业。该标准将安全概念分为功能与评估两部分。功能准则从 F1～F10 共分 10 级。1～5 级对应于 TCSEC 的 D 到 A。F6 至 F10 级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性和完整性的网络安全。

与 TCSEC 不同，它并不把保密措施直接与计算机功能相联系，而是只叙述技术安全的要求，把保密作为安全增强功能。另外，TCSEC 把保密作为安全的重点，而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。ITSEC 定义了从 E0 级（不满足品质）到 E6 级（形式化验证）的 7 个安全等级，对于每个系统，安全功能可分别定义。

18.2.3 CTCPEC

CTCPEC（Canadian Trusted Computer Product Evaluation Criteria）是加拿大的评价标准，专门针对政府需求而设计。与ITSEC类似，该标准将安全分为功能性需求和保证性需要两部分。功能性需求共划分为四大类：机密性、完整性、可用性和可控性。每种安全需求又可以分成很多小类，来表示安全性上的差别，分级条数为0～5级。

18.2.4 FIPS

美国商业部长依据信息技术管理改革法，批准NIST（ National Institute of Standards and Technology，技术与标准国家协会）为联邦计算机系统制定的标准和指南。

NIST 发布这些用于政府领域的标准和指南作为联邦信息处理标准（Federal Information Processing Standards，FIPS）。NIST制定FIPS用于没有现成工业标准和方案可以满足的联邦政府强制性要求，例如：安全和通用性。联邦信息处理标准（Federal Information Processing Standards，FIPS）是一套描述文件处理、加密算法和其他信息技术标准（在非军用政府机构和与这些机构合作的政府承包商和供应商中应用的标准）的标准。

18.2.5 BS7799系列（ISO/IEC 27000系列）

1. BS7799第一部分

BS7799第一部分的全称是Code of Practice for Information Security，即信息安全的实施细则。2000年被采纳为ISO/IEC 17799，目前其最新版本为2005版，也就是ISO 17799:2005。

ISO/IEC 17799:2005 通过层次结构化形式提供安全策略、信息安全的组织结构、资产管理、人力资源安全等11个安全管理要素，还有39个主要执行目标和133个具体控制措施（最佳实践），供负责信息安全系统应用和开发的人员作为参考使用，以规范化组织机构信息安全管理建设的内容。

2. BS7799 第二部分

BS7799第二部分的全称是Information Security Management Specification，即信息安全管理体系规范，其最新修订版在2005年10月正式成为ISO/IEC 27001:2005，ISO/IEC 27001是建立信息安全管理体系（ISMS）的一套规范，其中详细说明了建立、实施和维护信息安全管理体系的要求，可用来指导相关人员去去应用 ISO/IEC 17799，其最终目的在于建立适合企业需要的信息安全管理体系（ISMS）。

18.2.6 ISO/IEC TR 13335 系列

ISO/IEC TR 13335，早前被称作“IT 安全管理指南”（Guidelines for the Management of IT Security，GMITS），新版称作“信息和通信技术安全管理”（Management of Information and Communications Technology Security，MICTS），是 ISO/IEC JTC1 制定的技术报告，是一个信息安全管理方面的指导性标准，其目的是为有效实施 IT 安全管理提供建议和支持。

ISO/IEC TR 13335 系列标准（旧版）——GMITS 由 5 部分标准组成。

1．ISO/IEC13335-1:1996《IT 安全的概念与模型》
2．ISO/IEC13335-2:1997《IT 安全管理与策划》
3．ISO/IEC13335-3:1998《IT 安全管理技术》
4．ISO/IEC13335-4:2000《防护措施的选择》
5．ISO/IEC13335-5:2001《网络安全管理指南》

目前，ISO/IEC 13335-1:1996 已经被新的 ISO/IEC 13335-1:2004（MICTS 第 1 部分：信息和通信技术安全管理的概念和模型）所取代，ISO/IEC 13335-2:1997 也将被正在开发的 ISO/IEC 13335-2（MICTS 第 2 部分：信息安全风险管理）取代。

ISO/IEC TR 13335 只是一个技术报告和指导性文件，并不是可依据的认证标准，信息安全体系建设参考 BS 7799，具体实践参考 ISO TR 13335。

18.2.7 SSE-CMM

SSE-CMM（System Security Engineering Capability Maturity Model）模型是 CMM 在系统安全工程这个具体领域应用而产生的一个分支，是美国国家安全局（NSA）领导开发的，是专门用于系统安全工程的能力成熟度模型。

SSE-CMM 第一版于 1996 年 10 月出版，1999 年 4 月 SSE-CMM 模型和相应评估方法 2.0 版发布。

系统安全工程过程一共有 3 个相关组织过程。

1．工程过程
2．风险过程
3．保证过程

系统安全工程共分 5 个能力级别和 11 个过程区域，能力级别如下。

1．基本执行级
2．计划跟踪级
3．充分定义级
4．量化控制级
5．持续改进级

2002 年，SSE-CMM 被国际标准化组织采纳成为国际标准即 ISO/IEC 21827:2002《信息技术系统安全工程－成熟度模型》。

SSE-CMM 和 BS7799 都提出了一系列最佳惯例，但 BS7799 是一个认证标准（第二部分），提出了一个可供认证的 ISMS 体系，组织应该将其作为目标，通过选择适当的控制措施（第一部分）去实现。而 SSE-CMM 则是一个评估标准，适合作为评估工程实施组织能力与资质的标准。

18.2.8 ITIL 和 BS15000

ITIL 的全称是信息技术基础设施库（Information Technology Infrastructure Library）。ITIL 针对一些重要的 IT 实践，详细描述了可适用于任何组织的全面的清单（Checklists）、任务（Tasks）、程序（Procedures）、 职责（Responsibilities）等。

IT 服务管理中最主要的内容就是服务交付（Service Delivery）和服务支持（Service Support）

（1）服务交付包括以下内容。

- ❑ 服务级别管理（Service Level Management）
- ❑ IT 服务财务管理（Financial Management for IT Service）
- ❑ 能力管理（Capacity Management）
- ❑ IT 服务连贯性管理（IT Service Continuity Management）
- ❑ 可用性管理（Availability Management）

（2）服务支持包括以下内容。

- ❑ 服务台（Service Desk）
- ❑ 事件管理（Incident Management）
- ❑ 问题管理（Problem Management）
- ❑ 结构管理（Configuration Management）
- ❑ 变动管理（Change Management）
- ❑ 发布管理（Release Management）

英国标准协会（British Standard Institute，BSI）在国际 IT 服务管理论坛年会上，正式发布了基于 ITIL 的英国国家标准 BS15000。2002 年，BS15000 为国际标准化组织（ISO）所接受，作为 IT 服务管理的国际标准的重要组成部分。BS15000 有两个部分。

（1）ISO/IEC 20000-1:2005 信息技术服务管理—服务管理规范（Information technology service management. Specification for Service Management）

（2）ISO/IEC 20000-2:2005 信息技术服务管理—服务管理最佳实践（Information technology service management. Code of Practice for Service Management）

而与 BS7799 相比，ITIL 关注面更为广泛（信息技术），而且更侧重于具体的实施流程。信息安全管理体系（ISMS）实施者可以将 BS7799 作为 ITIL 在信息安全方面的补充，同时引入 ITIL 流程的方法，以此加强信息安全管理的实施能力。

目前，IT 服务管理（ITSM）领域正成为全球 IT 厂商、政府、企业和业界专家广泛参与的新兴领域，对未来的 IT 走向和企业信息化，将会产生深远的影响。其内容描述的是 IT 部门应该包含的各个工作流程以及各个工作流程之间的相互关系。

ITIL 包括了一系列适用于所有 IT 组织的最佳实践--无论这些组织的规模如何，以及

使用的是什么技术。事实上，这 15 年来的发展，ITIL 在全球，尤其是欧美地区一直是如火如荼。它已经被全球近 20000 多家在不同领域和行业领先的组织不同程度上所使用。需要强调的一点是：ITIL 不是一个正式标准，而是目前普遍实行的“事实”上的标准。

18.2.9 CC

通常所称的通用标准或通用准则（Common Criteria，CC）是指 ISO/IEC15408:1999 标准。目前 CC 标准的最新版本是 2.2；CC2.1 版在 1999 年成为国际标准 ISO/IEC15408:1999；我国在 2001 年等同采用为国家标准 GB/T 18336－2001。

CC 标准由 3 个部分组成。

（1）GB/T 18336.1－2001 idt ISO/IEC15408-1:1999 信息技术安全技术信息技术安全性评估准则第 1 部分：简介和一般模型。

（2）GB/T 18336.2－2001 idt ISO/IEC15408-2:1999 信息技术安全技术信息技术安全性评估准则第 2 部分：安全功能要求。

（3）GB/T 18336.3－2001 idt ISO/IEC15408-3:1999 信息技术安全技术信息技术安全性评估准则第 3 部分：安全保证要求。

如图 18-3 所示，与 BS7799 标准相比，CC 的侧重点放在系统和产品的技术指标评价上，BS7799 在阐述信息安全管理要求时，并没有强调技术细节。因此，组织在依照 BS7799 标准来实施 ISMS 时，一些牵涉系统和产品安全的技术要求，可以借鉴 CC 标准。

GB/T 18336 CC	GB 17859	TCSEC	CTCPEC	ITSEC
		D	T-0	E0
EAL1		-	T-1	
EAL2	第一级	C1	T-2	E1
EAL3	第二级	C2	T-3	E2
EAL4	第二级	B1	T-4	E3
EAL5	第四级	B2	T-5	E4
EAL6	第五级	B3	T-6	E5
EAL7		A1	T-7	E6

图 18-3　CC 与其他标准的评测级别对应关系图

18.2.10 CoBIT

CoBIT 的全称是信息和相关技术的控制目标（Control Objectives for Information and related Technology），是 ITGI 提出的 IT 治理模型（IT Governance），是一个 IT 控制和 IT 治理的框架（Framework）。CoBIT 是一个在更高的层面上指导管理层进行技术标准和信息系统管理的 IT 治理模型。

CoBIT 的 8 个控制过程：计划和组织（Planning & Organisation）、采购和实施

（Acquisition & Implementation）、交付和支持（Delivery & Support）、监视和评估（Monitoring & Evaluation）。

CoBIT 的 7 个控制目标：机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、有效性（Effectiveness）、高效性（Efficiency）、可靠性（Reliability）、符合性（Compliance）。

目前基本上存在着两类控制模型，一类是类似 COSO 这样的商业控制模式（business control model），另一类则是像 BS7799 这样的更关注 IT 的控制模型（more focused on IT control model），而 CoBIT 的目标是在两者之间架起一座桥梁。

18.2.11 NIST SP800 系列

美国国家标准技术协会（National Institute of Standards and Technology，NIST）发布的 Special Publication 800 文档是一系列针对信息安全技术和管理领域的实践参考指南，其中有多篇是有关信息安全管理的，包括以下内容。

- **SP 800-12** 计算机安全介绍（An Introduction to Computer Security: The NIST Handbook）。
- **SP 800-30** IT 系统风险管理指南（Risk Management Guide for Information Technology Systems）。
- **SP 800-34** IT 系统应急计划指南（Contingency Planning Guide for Information Technology Systems）。
- **SP 800-26** IT 系统安全自我评估指南（ Security Self-Assessment Guide for Information Technology Systems）。

这些文件可以作为实施 ISMS 过程中一些关键任务的指导和参照（例如风险评估、应急计划等），是对 BS7799 标准很好的补充和细化。

18.3 安全法规

信息安全法律法规是各种实践活动的指导和原则，尽管不是法律文本，也不是权威的法律顾问的替代品，但是对规范信息安全职业的法律法规有一个基本的了解还是很重要的。有一些法律规定了在信息系统中存储和处理信息的隐私权，另一些提供了各种行业所要求的安全防护的细节。

我国信息化法律法规建设与国家发展，尤其是与国家的法制建设进程是同步的，过程分为不同阶段：1949—2001 年间，信息化立法停留在分散立法阶段，主要是由国务院和各部门针对信息化发展中出现的一些突出问题通过制定法规和规章加以调整，重点集中在电子商务、信息安全、互联网治理等方面；2002 年至今处于集中立法阶段，立法作为全面推进信息化中的一项基础性工作，在电子签名与电子商务、政府信息公开、个人信息保护、信息安全保护以及互联网治理等领域得到极大发展，其中 2004 年 8 月通过的《电子签名法》是我国电子商务和信息化领域的第一部专门法律，2007 年 1 月通过的《政府信息公开条例》则第一次系统建立了规范的、可操作的政府信息公开制度。

下面列举了我国现阶段的一些信息安全方面的法律法规。

《互联网出版管理暂行规定》

《计算机信息系统保密管理暂行规定》

《计算机病毒防治管理办法》

《计算机信息网络国际联网出入口信道管理办法》

《计算机信息网络国际联网安全保护管理办法》

《公安部关于对与国际联网的计算机信息系统进行备案工作的通知》

《计算机信息系统安全专用产品检测和销售许可证管理办法》

《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》

《中华人民共和国计算机信息系统安全保护条例》

《商用密码管理条例》

《电子签名法》

习　　题

一、选择题

1. 常见的通用安全原则为特权分离原则、最小特权原则、深度防御原则以及下列哪一项？(　　)

A. 物理安全策略　　B. 人员安全策略

C. 区域安全策略　　D. 模糊安全策略

2. 数据管理策略不包括下列哪一项？(　　)

A. 最长保管时间　　B. 最短保管时间

C. 数据安全　　D. 数据类型

二、问答题

1. 简述最小特权原则的实施与重要性。

2. 简述通用安全管理工具减轻执行安全策略的过程。

3. 思考如何为一个组织或企业编写并执行具体的安全策略。

课 后 实 践

1. 了解并熟悉目前国际上通用的信息安全标准。
2. 熟悉 CC 标准的具体内容以及和其他标准的对应关系。
3. 了解我国在信息安全标准制定方面所做的工作和取得的进展。

第 19 章　构建企业安全实践

本章学习重点：

- 为企业建立一个强健的安全计划
- 理解企业业务持续性计划重要性
- 实施灾难恢复计划
- 应用数据分类程序
- 安全法律法规

目前，并非所有组织都重视自身安全建设。作为一名安全从业人员，只能利用组织中有限的资源（经济上、人力上以及其他方面）来构建企业的安全，解决企业当中各种各样的问题。本章将介绍安全专家利用安全工具、技术手段和安全实践构建企业安全，完成组织业务目的的方法。

19.1　构建企业安全案例

对许多安全专家而言，构建企业安全案例是一项具有挑战性的任务。在很多企业中，企业人员和安全人员之间都存在分歧，消除这个分歧需要两方面的共同努力。

作为一名安全从业人员，必须要理解企业的各种意图。毕竟，所有程序（包括安全程序）都是为了支持企业的最终目标。安全人员首先要对企业的目标有一个整体的了解，然后决定如何在实现这些目标的过程中保护企业的安全。在较小的公司里，安全人员只需和相关人员进行交谈，阅读一些企业相关的书面材料就能达到这个目的。在大型企业里，则需要更多的措施来构建企业知识库。另外，如果负责的部门是特定的企业单元，就需要对这个单元业务操作的细节有详细的了解。

有两种类型的风险分析方法：定性分析方法和定量分析方法。当建立企业安全案例的时候，可以使用相似的方法。企业管理者考虑企业决策的时候，很多时候是以单纯的定量方法进行的（例如，一种新的垃圾邮件过滤工具每年能够节省 1000 个工作时，每个工作时的平均成本是 15 美元，因此，这个过滤工具每年节省的是 15000 美元。而这个过滤器工具的成本只有 5000 美元，所以选择使用这个垃圾邮件过滤工具）。另外一些企业决定是由定性方法做出的（例如，防火墙可以阻止入侵者进入企业网络偷走商业秘密，而这些秘密如果被泄露给竞争对手，会造成整个企业的重大损失。所以，无论花费多大的代价，企业必须应用防火墙）。在构建企业案例的时候，要考虑到程序应用后对企业可能的结果，这样可以帮助选择合适的策略。

在构建企业安全实践的时候，要学习一些企业业务相关的课程。学习一些有关会计、金融及企业管理战略部署的知识，可以更好地帮助理解企业的整体功能。同时要掌握一些企业管理人员使用的专业术语，这样可以有效地和相关人士进行交流。

19.2 企业业务连续性计划

每一个组织都面临着风险。火灾、洪水、盗窃、战争以及其他事故威胁着每个企业的连续性运作。信息安全专家的一项重要责任就是保护企业计算机资源免受这些风险的威胁。这种实践被叫做企业业务连续性计划，其核心就是要开发，应用并维护企业组织的业务连续性计划（BCP）。

下面的内容，将要讨论制订企业业务连续性计划最主要的几点注意事项，包括最初的漏洞评估、安全控制手段的实施等。

19.2.1 漏洞评估

每个企业都面临着大量的信息安全漏洞。其中一些是技术上的风险，例如黑客、硬件错误以及操作错误。另一些则是间接的威胁，例如自然灾害和建筑物倒塌。为有效管理风险，组织必须找出潜在的风险并采取一定的措施进行弥补，注意不要在一些无足轻重的事件上花费太多的时间。一个位于内陆地区的公司不应该把大量的时间花费在预防海啸的发生。

漏洞评估是建立组织 BPC 的第一步。通过这个初步分析找出组织中存在的漏洞，并决定漏洞相应的威胁以及构成的重大风险。经常用一个公式来表达这些概念之间的关系：

$$风险=威胁\times漏洞$$

通过一个例子对这个公式进行解释。假如一个公司位于海岸线上，但并没有建立海堤。如果发生海啸，那么整个建筑就会被全部破坏掉。因此，公司的漏洞是非常大的。然而，在公司地点发生海啸的可能性却是非常低的。因此，相乘之后，公司受海啸影响的风险是很低的。以同一个企业做例子。企业对洪水的漏洞是很高的。同时，发生洪水可能性也是很高的。等式的两个因子很高，结果是风险也很高，这就需要企业业务连续性计划者给予重视。

图 19-1 给出了一个象限图，用户可以在图中描绘自己的计算结果，包括了海啸和洪水的例子。当风险落在第一象限时，就要求更多的注意。风险位置越靠近右上部，就越需要更多的注意。对第二，第三象限的风险应该进行分析，并且要采取一定的控制手段。落在第四象限的风险，尽管不能完全忽视，但基本不会对组织构成太大的风险。

19.2.2 实施控制

有 4 种管理风险的技术：风险规避（risk avoidance）、风险降低（risk mitigation）、风险接受（risk acceptance）以及风险转移（risk transference），当然也可以综合使用 4 种方法。在风险分析和漏洞评估过程中，企业的安全团队会给出处理每种风险的策略。BPC 的目标就是对策略进行分析，并将其具体化为可被执行的条款。用户面对的一些技术上的风险可以通过使用技术控制手段（例如访问控制系统、防火墙和入侵检测系统）来减轻。其他的风险可以综合教育、培训以及监视系统等手段来减轻。另外，一些物理风险（例如由洪水构成的风险）需要其他学科的专家（例如工程师和建筑师）来处理。

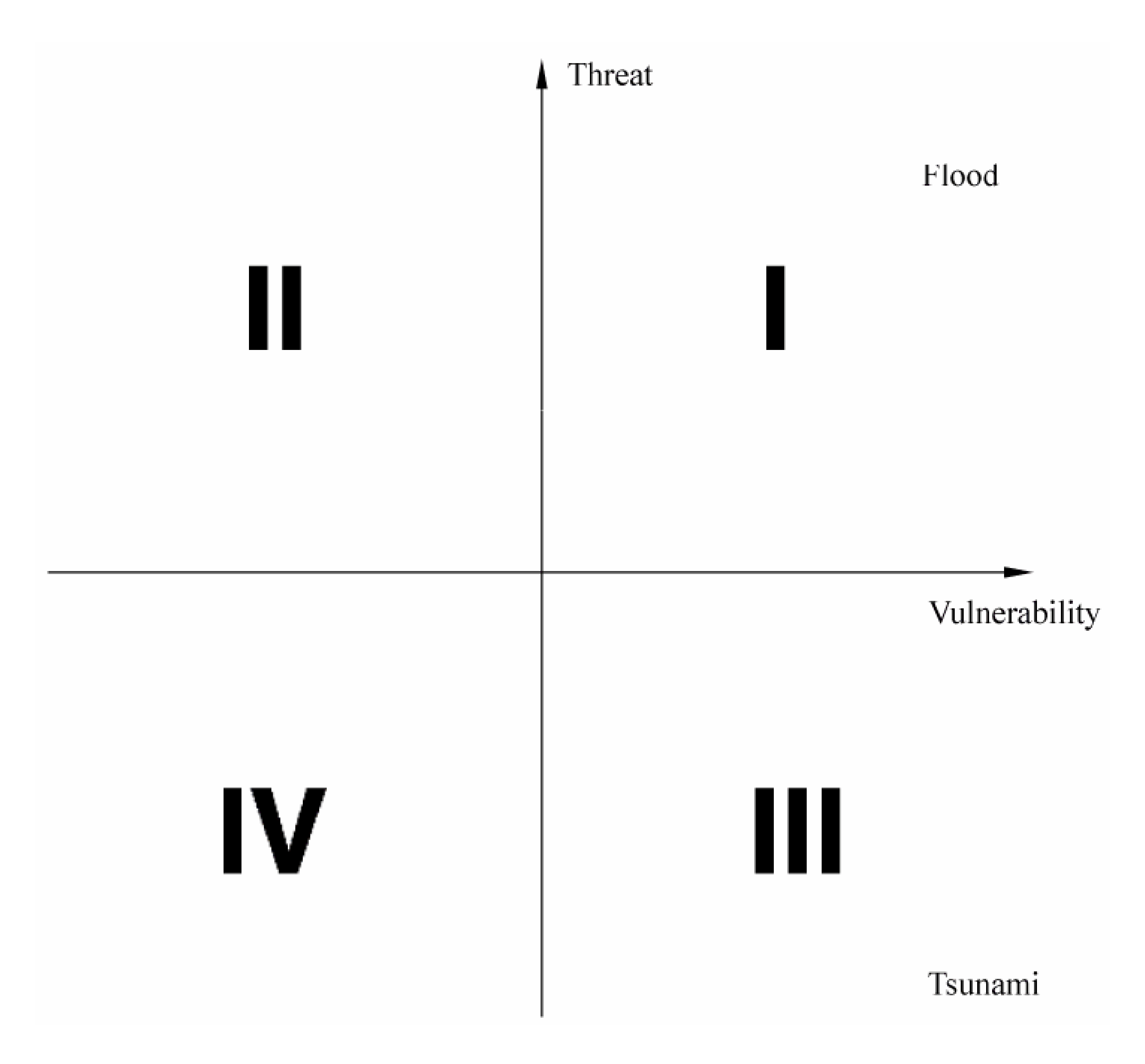


图 19-1　风险评估象限图

19.2.3　计划维护

BPC 是一个动态文件。随着组织的不断变化，组织所面临的风险也会不断改变。要定期召开 BPC 开发和维护人员的会议，保证组织和环境中的变化能够被合理处理，不会影响企业连续性控制要求。当变化发生的时候，BPC 必须要能够进行灵活调整以适应新发生的变化。

19.3　灾难恢复计划

组织运用灾难恢复计划应对灾难发生导致的组织操作被打断的情况。这个过程通常由灾难恢复计划（DRP）的文档来描述。DRP 有以下 3 个主要目标。

（1）灾难发生时，快速替换处理设施保证生产的连续性。

（2）为替换设施提供操作维护。

（3）灾难解决之后，帮助组织快速恢复原有设备的生产操作。

19.3.1　选择维护团队

灾难恢复计划最重要的一步就是选择一支专业的灾难恢复团队。在规模较小的组织里，这个团队由少量的成员组成，担任着 DRP 开发和维护的任务，并且在灾难发生时负责计划的切实执行。在规模较大的组织中，一般有两种类型的 DRP 成员。首先要有由来

自于企业各个职能部门的重要代表构成的一个中央委员会，负责 DRP 开发和维护的全部任务。然而，在灾难发生的实际过程中，由这个委员会负责所有的计划实施任务是不可行的。因此，还要有另外一些员工进行，保证计划顺利执行。DRP 组成员在组织内部的 DRP 角色只是他们的次要角色。在组织正常运作期间，他们正常工作职能是放在第一位的。

19.3.2 制订灾难恢复计划

选择灾难恢复团队后，接下来是设计 DRP。用户应当确保在设计计划的核心团队中包括了企业中所有重要部门的代表。DRP 应该描述在灾难发生时如何以一种有序的方式将业务转移到恢复设备中。应该把灾难恢复计划组成员的责任具体化，并且要同时列出执行计划时所需要的资源和灾难恢复设备。这些资源包括以下内容。

- **资金资源** 现金支出是执行这个计划所必须的。
- **人力资源** 来自于整个组织内部的员工需要把他们大部分或全部的时间用于灾难恢复工作。
- **硬件资源** 在灾难恢复现场可能会需要信息处理系统。
- **软件资源** 对于企业的持续运转，软件和数据是非常重要的，必须及时传送给灾难恢复设备。

选择灾难恢复设备是灾难恢复计划人员面临的重要挑战，主要有 3 种地方放置灾难恢复设备。

- **热门地点（Hot sites）** 包括了恢复业务运行所必需的全部硬件、软件和数据。灾难发生后，这些地点能够立刻接管生产任务。
- **一般地点（Warm sites）** 包括了恢复业务运行所必需的大多数硬件、软件资源。灾难发生后，可能需要几个小时或是几天的时间从备份中下载导入数据以恢复组织的全部处理功能。
- **冷门地点（Cold sites）** 并没有运行企业业务所必需的硬件、软件和数据资源，只是维护着企业运行必须的支持系统（电力、热力、空调设施、安全设备等）和传送业务必须的通信线路。冷门地点通常需要大量时间来激活（通常以星期或月来衡量）。

19.3.3 培训和测试

一旦用户为自己的组织制定了合适的 DRP，就必须建立一项培训计划保证所有和 DRP 有关的人员熟悉计划激活时自己所承担的职责。大多数的组织通常结合多种方法来实施 DRP 培训，其中包括以下两种培训方法。

- **初始培训** 当某人刚进入组织内部的灾难恢复部门时，要进行这种培训。这种全面培训详细地介绍了每一个人明确的安全责任，提供了关于 DRP 的概述。
- **复习培训** 贯穿于雇员在企业工作的整个过程中。这种培训用来提醒员工的灾难恢复责任，保证他们已经做好了在灾难中断的企业业务运作中发挥作用的准备。

这种教育培训方法和一般安全策略培训很类似。培训项目的长度、频率以及范围应该根据每个人在 DRP 中所承担的责任来进行定制。

除了正式的 DRP 培训项目，灾难恢复团队应该对 DRP 进行周期性的检测。下面给出了常见的 DRP 检测：行动列表检查、桌面练习、软件测试及硬件测试。

1．行动列表检查

行动列表检查是最简单的一种 DRP 检测。行动列表为灾难响应小组的成员提供了行动指导。行动列表检测过程中，灾难恢复团队的目的有两个：明确自己所执行任务的细节；检查计划是否满足组织当前的业务需要。

组织的行动列表检查有不同的方式。一种是要求整个灾难恢复团队聚在一起执行检查过程。另一种是根据员工的 DRP 角色及企业角色分小组进行。在实际中，行动列表检查是基于个人基础进行的，应按照一定的规程并及时给出反馈，以进一步对列表进行修改。

2．桌面练习

更深层次的 DRP 检测是桌面练习。在这种检测中，灾难恢复团队成员一起叙述一个特定的灾难情景。通常情况下，主持人会描述一个假设的灾难情景，参加者就灾难发生时应该做成的行动给出讨论。这些讨论使团队成员有机会考虑很多特定的情景以及在特定场景下应该采取的措施。

3．软件测试

软件测试，比桌面练习的程度更深了一步。在这种评估中，灾难恢复团队成员对灾难做出实际响应，并且真正激活组织的灾难恢复设备。送往设备的数据流被激活，但是恢复场所并不承担组织的全部操作责任。这个站点仅仅是在特定的时间段内同生产设备同时运行。

软件测试真正测试了将要在灾难处理过程中被使用的硬件和软件资源，给出了 DRP 中描述的操作过程在实际应用中的反馈，但同时也增加了成本。软件测试要求在时间和资源上有更多的投资。

4．硬件测试

硬件测试，有时又被称为完全中断测试，对企业的影响最大，因此很少被使用。在这种类型的测试中，灾难恢复团队关闭运行的生产设备，尝试在灾难恢复设备上恢复运行操作。测试结束的时候，团队将控制交回给生产设备，模拟灾难真正发生时的过程。

尽管硬件测试极其昂贵，对企业运行所产生的影响十分巨大，但有时候仍然被一些组织所使用。这些组织的责任十分巨大，必须确保在真正的灾难发生之后能够成功恢复组织的运行。

19.3.4 实施计划

在企业的整个生命历程中，总会遇到某些意想不到的灾难发生。毫无疑问，在这个时候，企业的状况肯定是杂乱不堪的。企业员工很可能会质疑组织继续存在的能力，他们自己的生命和财产很可能会处于危险之中。所有这些情况要求用户的 DRP 应用规程必须是最有效最容易操作的。

DRP 计划应该定义出灾难第一响应人应该采取的行动。例如，一个程序员在收看新闻的时候看到一个附近的火山就要爆发，那么他就是灾难的第一响应人。当洪水正在冲击一座电厂的时候，值班人员就要负起灾难恢复的责任。组织里的每一个人当他们意识到自己最先注意到一场灾难即将发生的时候，都应当知道遵守的规程。

DPR 的应用可以对组织产生重大作用。因此，不能允许组织里的任意一个人独自宣布灾难的发生。通常是组织的高级管理人员可以做出这种判断，因此要保证能够随时联系到他们，从而快速做出决定。宣布灾难发生后，灾难恢复小组应该迅速集合，及时采取措施恢复组织运行。

19.3.5 计划的维护

灾难恢复计划是一个动态的计划，需要服从于企业的变化。灾难恢复小组的成员关系，行动规程，以及使用工具都会随着时间变化，DRP 应该足够灵活以适应这些变化。

灾难恢复小组应该依照行动列表和组织规程来建立。这样能够保证在突如其来的灾难面前采取冷静有效的措施。这些列表必须不断被更新。对灾难恢复计划进行维护最好的方法是不断地进行检测，使用各种技术对其进行评估。首先进行测试，然后不断总结在每一次测试的优点和不足，利用这些测试获得的珍贵反馈来执行 DRP 维护。

19.4 数据分类

数据分类系统向用户提供了一种将敏感信息分级的方法，并且以一种连续的方式向不同敏感程度的数据提供适度的保护。下面介绍了访问机密信息的两种预备知识，并且介绍了目前常见的两种分类系统。

19.4.1 安全许可

在一个使用数据分级程序的组织中，对于被授权访问机密信息人员最基本的要求就是必须要拥有安全许可。在一些组织中，确定安全许可是极其严格的过程，要求严格的背景调查、测谎测试以及安全契约的执行。在其他一些组织中，如果员工同意了保密契约，安全许可就能够根据职位自动被授予。

安全许可通常有不同的层次，明确指出了一个用户被授权访问的信息的最大敏感程度。安全许可同样授予一部分特殊的人可以访问特定的敏感数据。

安全许可应该只被授予那些极其需要来完成正常指定工作的人。另外，应该定期检查组织分支的许可状态。如果一个人不需要访问机密信息来完成他的工作，访问权限就应该被撤销，直到被重新需要为止。

19.4.2 必备知识

安全许可只是访问机密信息的两个必要条件之一。第二个是用户需要知道为了完成特定的工作任务需要哪些具体的机密信息。尽管安全许可提供了访问大量机密信息的权限（例如，所有的“秘密”数据），但是内容须知（need-to-know）把访问的范围缩小到了完成任务所必须的那部分内容上。

通常，安全许可的实施过程发生在组织的中心地点（通常是安全办公室）。这个办公室负责授予、维护以及撤销安全许可。然而，内容须知的确定通常是由负责监管特定机密信息的个人来执行的。当被要求访问机密信息时，监管者必须确定访问者的身份，核实他们的安全许可，决定这个人是否具有正当的需求可以访问想要获知的信息。如果访问者对内容须知一无所知，监管者就必须拒绝这样的访问。

19.4.3 分类系统

有两种主要的数据分类系统——一种用在政府部门，另一种用在个人企业中。大多数情况下，政府部门使用的分类系统比私人企业使用的分类系统的限制性更强。

1. 政府数据分类系统

美国政府使用强制访问控制系统。每一份机密资料被分配一个特定的安全等级，根据不同的安全等级为其提供适度的安全保护。美国政府将机密信息分为 5 级，分别如下。

- **绝密（Top Secret）** 这个级别的信息一旦泄露，会对国家安全造成异常严重的破坏。
- **秘密（Secret）** 信息一旦泄露，会对国家安全造成严重破坏。
- **机密（Confidential）** 信息一旦泄露，会对国家安全造成破坏。
- **敏感（sensitive but Unclassified）** 这种信息的泄露不一定会对国家的安全造成破坏，但政府却应该对其进行保护。例如，个人税收记录、部分公开的企业信息以及合同谈判的细节信息等。
- **公开（Unclassified）** 不需要保护，可以自由分配的信息。

2. 企业数据分类系统

企业数据分类系统通常不如政府分类系统复杂，但同样具有分级系统和访问控制。企业数据级别分为以下 4 种。

- **商业秘密（Trade Secret）** 构成组织核心秘密的信息。这类信息通常不受正式知识产权系统的保护（例如专利、著作权），相反，企业的管理者使用内部控制来保护这些信息免受非授权的泄露。

- **公司机密（Company Confidential /Proprietary）** 指那些企业不希望发放到公共领域的信息，但敏感性比商业秘密信息差一点。
- **公开信息（Unclassified）** 公司不要求保护的信息，可以向外界公开。

坚持对信息进行合理分类是非常重要的。尤其在自身知识产权维护的事件中。例如，公司认为某条信息是商业机密，但并没有明确地标注出来，那么一个前任员工就可以把这条信息透漏其他人，然后宣布并不知道这是一个商业机密。

习　　题

一、选择题

1. 常见的 DRP 检测类型有清单检查、软件测试、硬件测试以及下列哪一项？（　　）

A．前期培训　　B．桌面练习

C．初始训练　　D．复习训练

2. 灾难恢复的 3 种主要替换处理设施不包括下列哪一项？（　　）

A．热门地点　　B．冷门地点

C．安全地点　　D．一般地点

二、问答题

1．简述企业业务持续性计划的影响。

2．简述灾难恢复计划如何恢复被灾难中断的服务。

3．思考如何建立一个坚固的企业案例。

课后实践与思考

Windows Server 2003 灾难恢复实例

通过 Windows Server 2003 的备份工具进行服务器数据的备份和还原操作，以便在服务器发生灾难后能够迅速有效的恢复。首先介绍服务器灾难的定义和灾难恢复的要求，演示利用备份工具进行备份和还原操作的方法，同时还介绍利用安全模式和故障恢复控制台来启动服务器，解决服务器软件故障的方法。

一、灾难恢复介绍

1．服务器灾难

服务器灾难是指服务器由于硬件或存储媒体软件的突发故障而导致发生灾难性的数据丢失，可能如下。

- 操作系统无法启动。
- 用户数据文件丢失或已被破坏。
- 在安装新的应用程序之后，系统不稳定或应用程序运行不正常。
- 在更新硬件设备驱动程序之后，用户虽然可以登录，但系统不稳定。
- 在安装新的硬件设备之后，系统不稳定。

2．灾难恢复过程

- 执行书面的灾难恢复计划。
- 更换任何损坏的硬件。

- ❑ 恢复数据。
- ❑ 恢复运行前，测试全部硬件和软件。

3．准备灾难恢复的指导方针

- ❑ 创建灾难恢复计划以执行定期备份操作。
- ❑ 测试备份文件和备份计划。
- ❑ 保留两个备份集：一个在现场，易于访问；一个在异地，保证安全。
- ❑ 创建一个系统状态数据的冗余副本。

二、数据备份

数据和信息是网络中最有价值的部分，如果能够做到定期及时的备份数据，那么在发生数据丢失时，可以用还原功能及时恢复数据，把损失减少到最低。

1．备份的概念

所谓数据备份就是把数据从一个位置向另一个位置复制的过程。数据备份和第 5 章介绍的 RAID 容错都有在数据出错时恢复数据的功能，但两者是不同的概念。RAID 容错实际上是在硬盘上保留数据的冗余，冗余的数据没有经过任何处理，和原始数据完全一样，其好处是可以降低计算机发生故障的风险。备份是将重要数据保留在其他存储媒体上，如磁盘、磁带、光盘等，在备份过程中数据可以被压缩，当系统发生故障时通过还原功能将数据恢复到硬盘上。为了提高数据的安全性，重要数据还需要进行异地备份，以防止因为自然灾害等原因造成数据丢失。

2．备份的操作者

只有 Administrators、Backup operators 和 Server operator 组的成员允许备份本机数据。同时备份操作用户对硬盘的访问不能受磁盘配额的限制，否则将无法备份数据。

3．Windows 通过文件的存档属性判断是否需要备份

用于判断文件是否应该被备份。当文件创建或修改后，其存档属性被设置；一般来说，当它被备份后，存档属性被清除。

可以打开文件或文件夹的属性对话框，单击“常规”选项卡中的“高级”按钮，来查看其当前的存档属性，如图 19-2 所示。

4．备份类型

Windows Server 2003 提供了 5 种备份类型，满足不同的备份要求，包括正常备份、副本备份、增量备份、差异备份和每日备份。

（1）正常备份

普通备份主要用于备份所有选定的文件，而不考虑这些选定的文件是否被设置为存档属性，并且在完成备份之后清除这些文件的存档属性，即标记为已备份。

（2）副本备份

备份所有选定的文件，但不标记这些文件为已备份，即不清除文件的存档属性，所以可以在副本备份后，对文件执行其他备份。

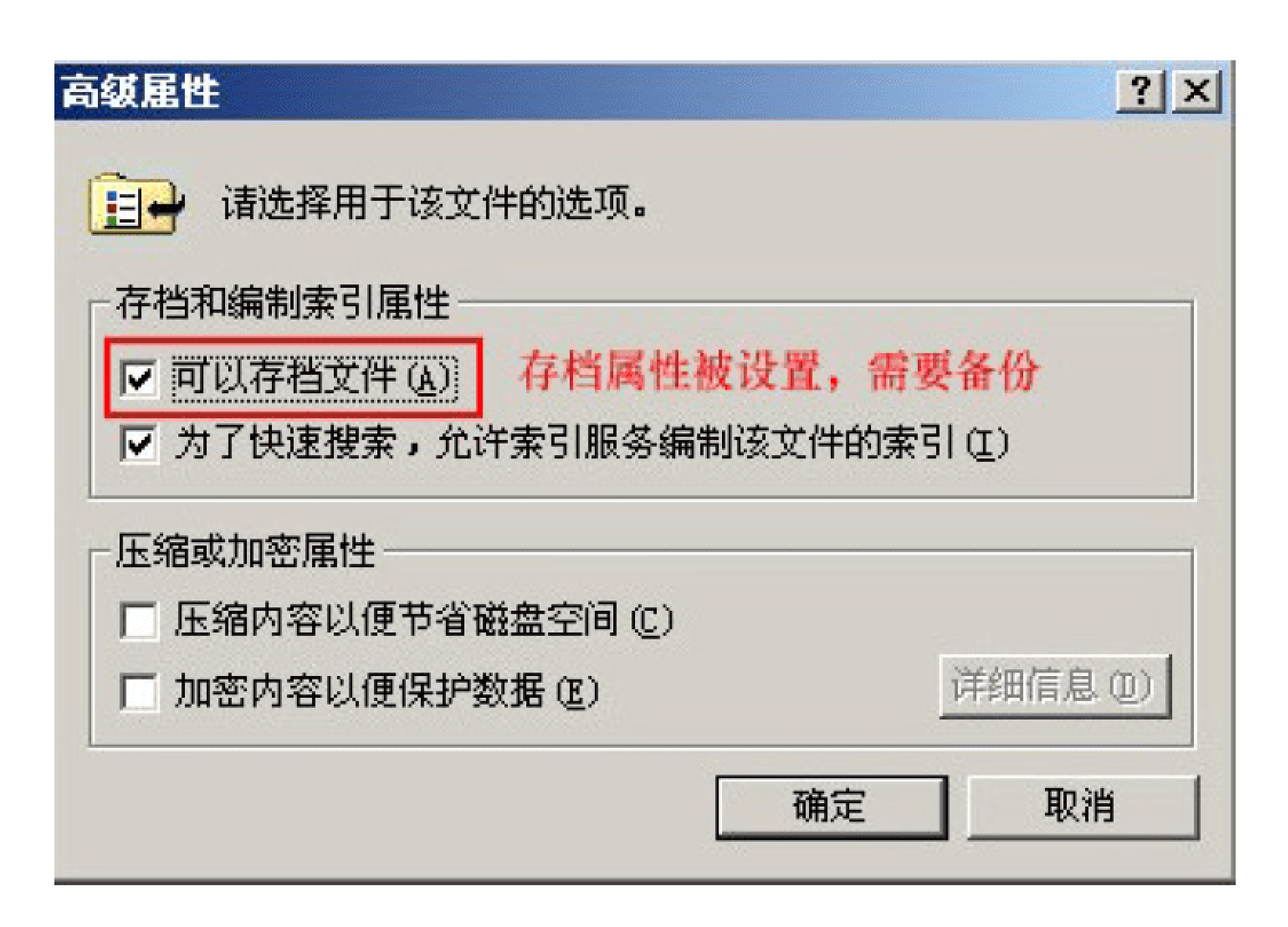


图 19-2　高级属性

（3）增量备份

备份自上次正常或增量备份以来新创建或修改的文件，并标记文件为已备份。因此该备份方法所需要的存储空间最少，并节省备份时间。通常和正常备份结合使用，恢复时需要正常备份集和所有之后的增量备份集。

（4）差异备份

用于备份自上次正常或增量备份以来所新创建或修改的文件，不清除文件的存档属性，即不标记文件为已备份。和正常备份结合使用，恢复时需要正常备份集和最后一次差异备份集。

（5）每日备份

备份当天更改过的所有选定文件，备份不清除文件的存档属性，即不将备份后的文件标记为已备份。

5．备份策略

进行数据备份时，希望能尽量少的占用服务器和网络资源；在进行数据还原时，希望能尽量在最短的时间内完成。不同的备份类型有不同的特点和长处，有的备份方法在备份数据时会花较多的时间，但在还原数据时花的时间较少；而有的备份方法则正好相反。在实际工作中，要根据备份的数据量、重要性、备份周期等来确定合适的备份策略。好的备份策略是几种备份方法的组合。

（1）正常备份+增量备份

情景描述：小张需要对服务器的数据进行备份，但备份用的磁盘空间比较紧张，且服务器比较可靠，还原操作比较少用。所以他希望能采用一种比较节约磁盘空间和备份时间的备份策略。

备份方案：周一进行一次正常备份，周二至周五每天进行一次增量备份。

恢复时：先恢复周一数据，再按顺序恢复每天的增量备份数据。

优点：节约存储空间和备份时间。

缺点：恢复时操作复杂。

（2）正常备份+差异备份

情景描述：小张需要对服务器的数据进行备份，考虑到可能要经常进行还原操作。所以他希望能采用一种还原操作很方便的备份策略。

备份方案：周一进行一次正常备份，周二至周五每天进行一次差异备份。

恢复时：先恢复周一数据，再恢复最后一天的差异备份数据。

优点：恢复方便。

缺点：备份时需要较多的存储空间和时间。

6．备份操作

（1）手工备份

下面以备份 C:\Documents 文件夹为例介绍使用备份工具的步骤。

① 单击“开始”→“程序”→“附件”→“系统工具”→“备份”命令。

② 选择高级模式，在其中选择“备份向导”，如图 19-3 所示。

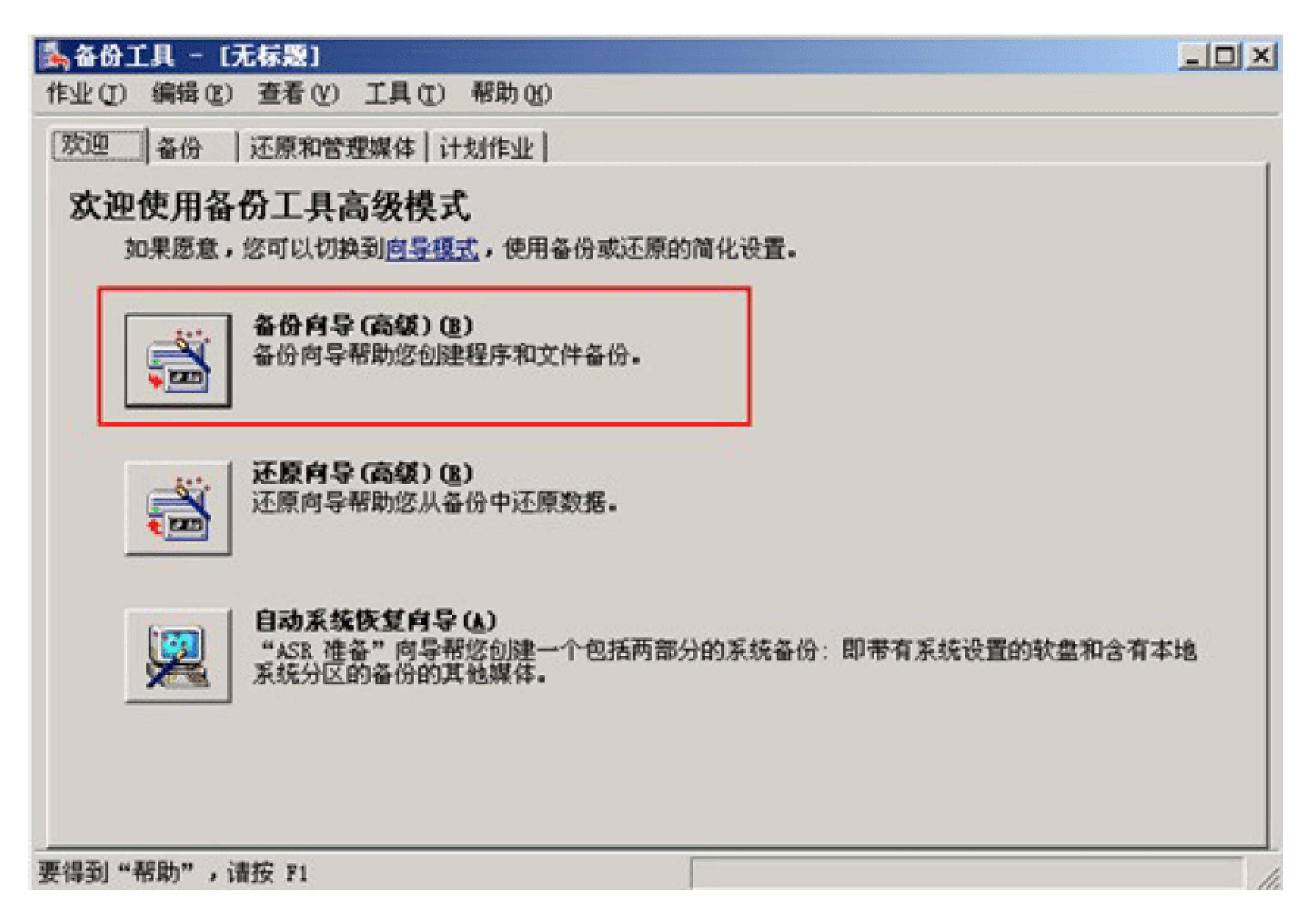


图 19-3　选择“备份向导”

③ 如图 19-4 所示，选择“备份选定的文件、驱动器或网络数据”单选按钮，然后选中需要备份的文件或文件夹。

④ 输入备份文件的存储位置和文件名。

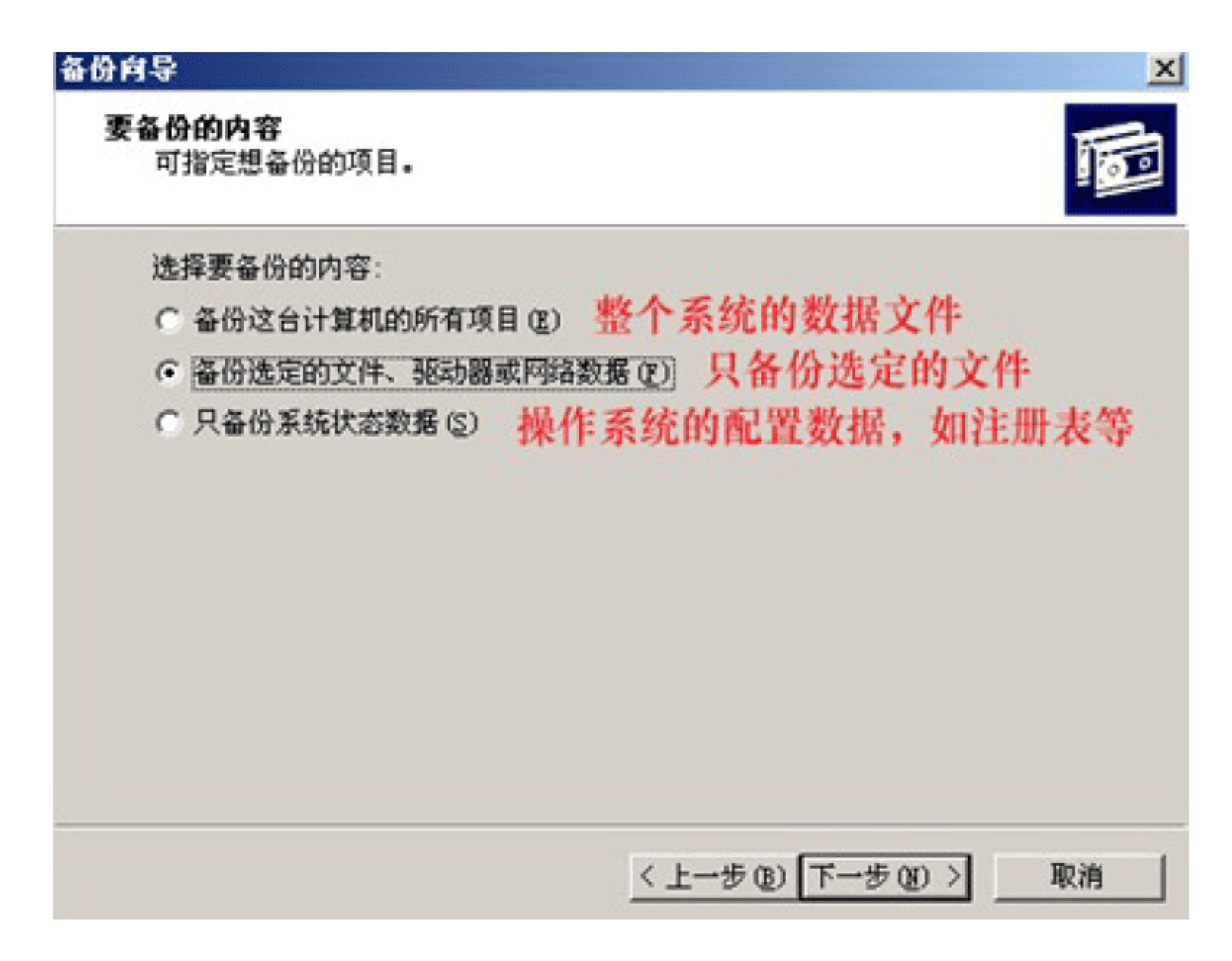


图 19-4　选择要备份的内容

⑤ 在“备份向导”对话框中，单击“高级”按钮，如图 19-5 所示。



图 19-5　完成备份向导

⑥ 选择备份类型。

⑦ 在如何备份中，决定备份后是否验证数据。

⑧ 在备份选项中，选择附加或替换原有的备份。

- **将这个备份附加到现有备份**　将本次备份的数据附加到上一次备份的数据之后，保存在同一个备份文件。

❑ **替换现有备份** 本次备份的数据将覆盖原来备份的数据。

⑨ 在备份时间中，选择现在进行备份。

注：也可以不使用向导，而直接在“备份工具”对话框中进行操作。此时可以在“工具”菜单的“选项”对话框中设置备份选项等。

（2）自动备份

情景描述：小张每天都要对服务器数据进行一次备份操作。如果用手工操作，费时费力，而且容易遗忘。

解决方案：利用备份工具的自动备份功能，每天在特定时间进行一次备份。

① 前期操作同手工备份中的 1～8，在第 9 步中选择“以后”单选按钮。

② 输入一个作业名，并单击“设定备份计划”按钮，如图 19-6 所示。



图 19-6　设置备份时间

③ 如图 19-7 所示，在“计划作业”对话框中，选择“每日”，并可单击“高级”按钮进行更多的设置；还可以在“设置”选项卡中进行进一步的管理。

④ 在“设置账户信息”对话框中，输入能够完成备份操作的用户的用户名和密码。

注：完成操作后，可以在系统的计划任务中看到建立的自动备份作业。

（3）还原操作

当系统发生故障或其他意外情况时，可以利用还原功能恢复以前备份的数据，这样可以减少损失。具体步骤如下。

① 在“备份工具”对话框中，选择“还原向导”。

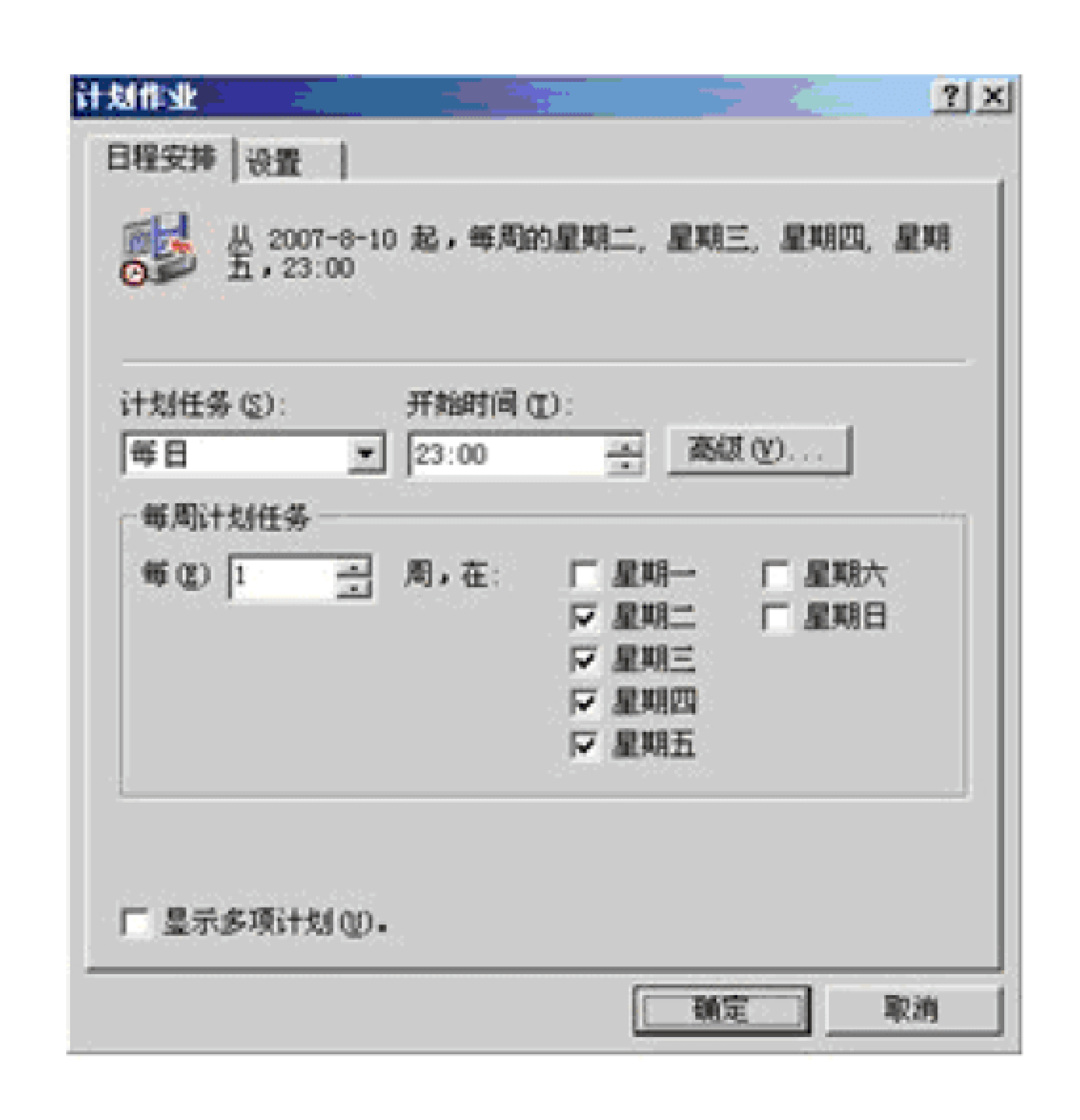


图 19-7　计划作业

② 选择要还原的文件和文件夹的目标位置，如图 19-8 所示。

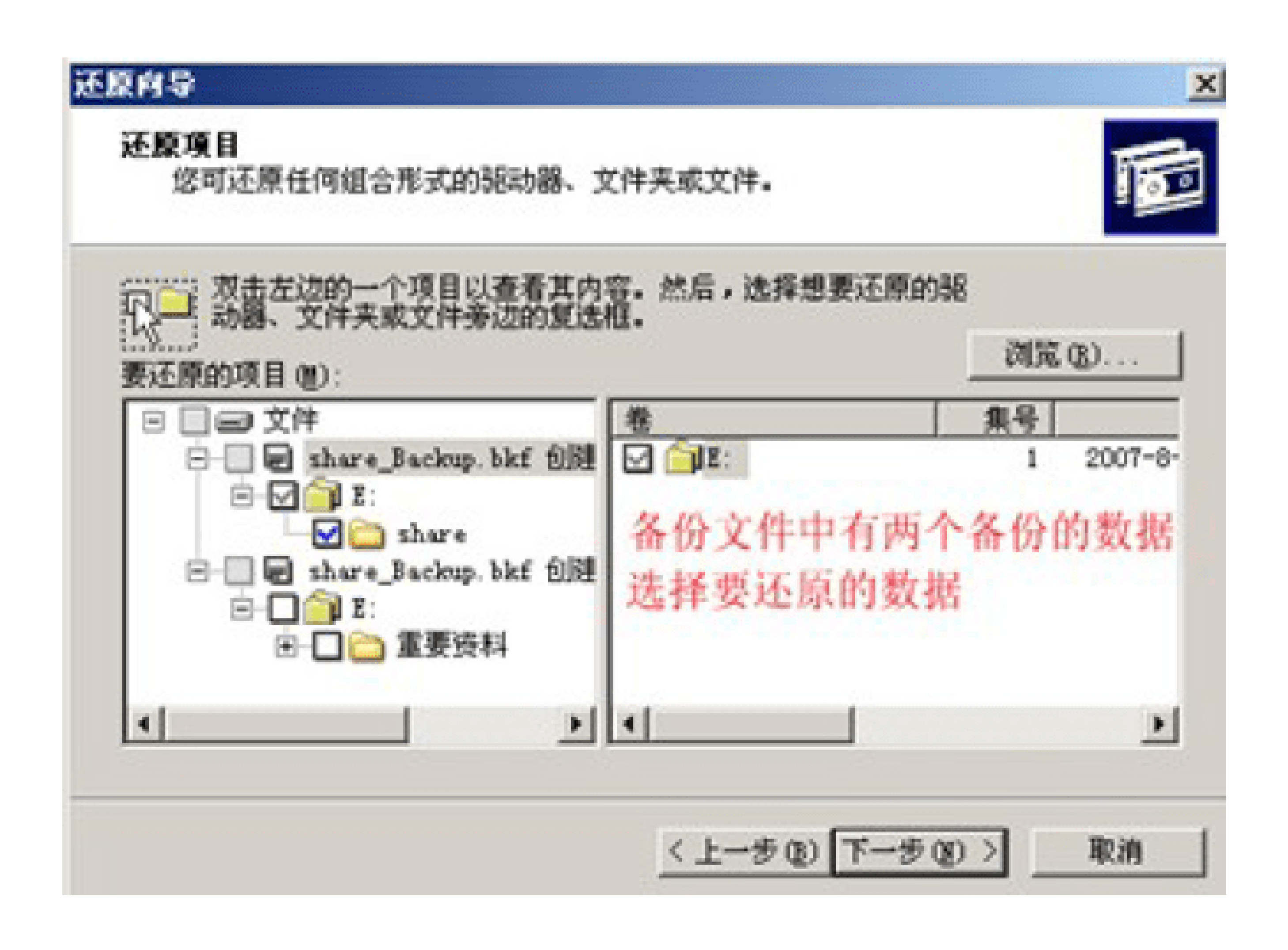


图 19-8　选择要还原的项目

③ 在完成对话框中，单击“高级”按钮，如图 19-9 所示。

④ 选择还原位置，如图 19-10 所示。

- **原位置**　将备份文件还原到原来的文件夹中。
- **备用位置**　将备份文件还原到另一个文件夹中。当用户不想改变原文件夹中的当前内容时可以使用此项。
- **单个文件夹**　将备份文件还原到单一文件夹中，不保留原来备份文件夹和文件的结构。



图 19-9 完成还原向导

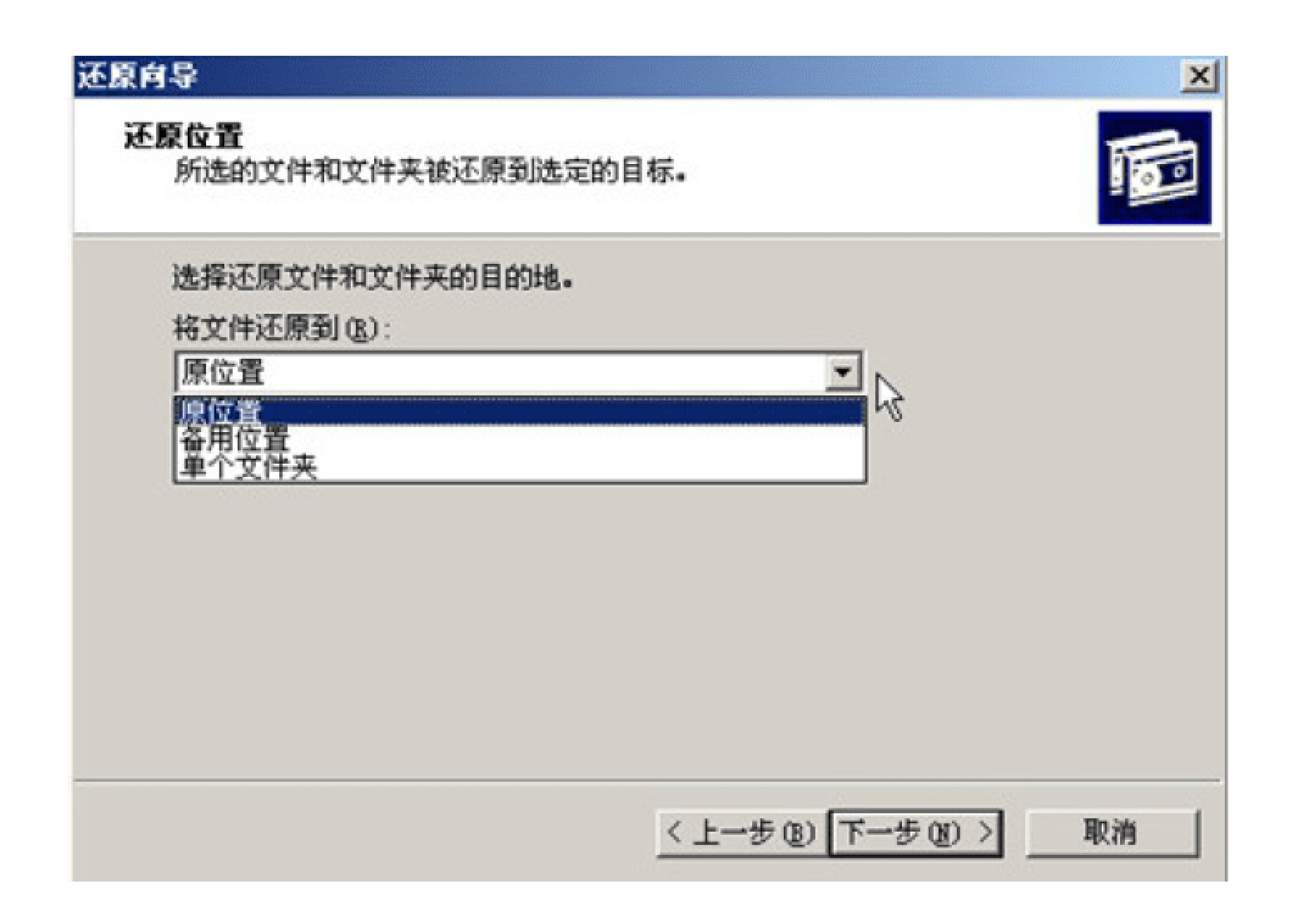


图 19-10 选择还原位置

⑤ 选择如何还原，如图 19-11 所示。

❑ **保留现有文件** 最安全的作法。

❑ **如果现有文件比备份文件旧，将其替换** 可以保证计算机上的是最新副本。

❑ **替换现有文件** 不保留现有的文件。

⑥ 当完成还原向导后，就会开始进行还原操作了，如图 19-12 所示。

（4）服务器故障恢复

当服务器因系统或用户操作错误而导致系统工作不正常甚至系统崩溃时，可以使用一些系统还原的方法来尝试让系统恢复到正常状态。

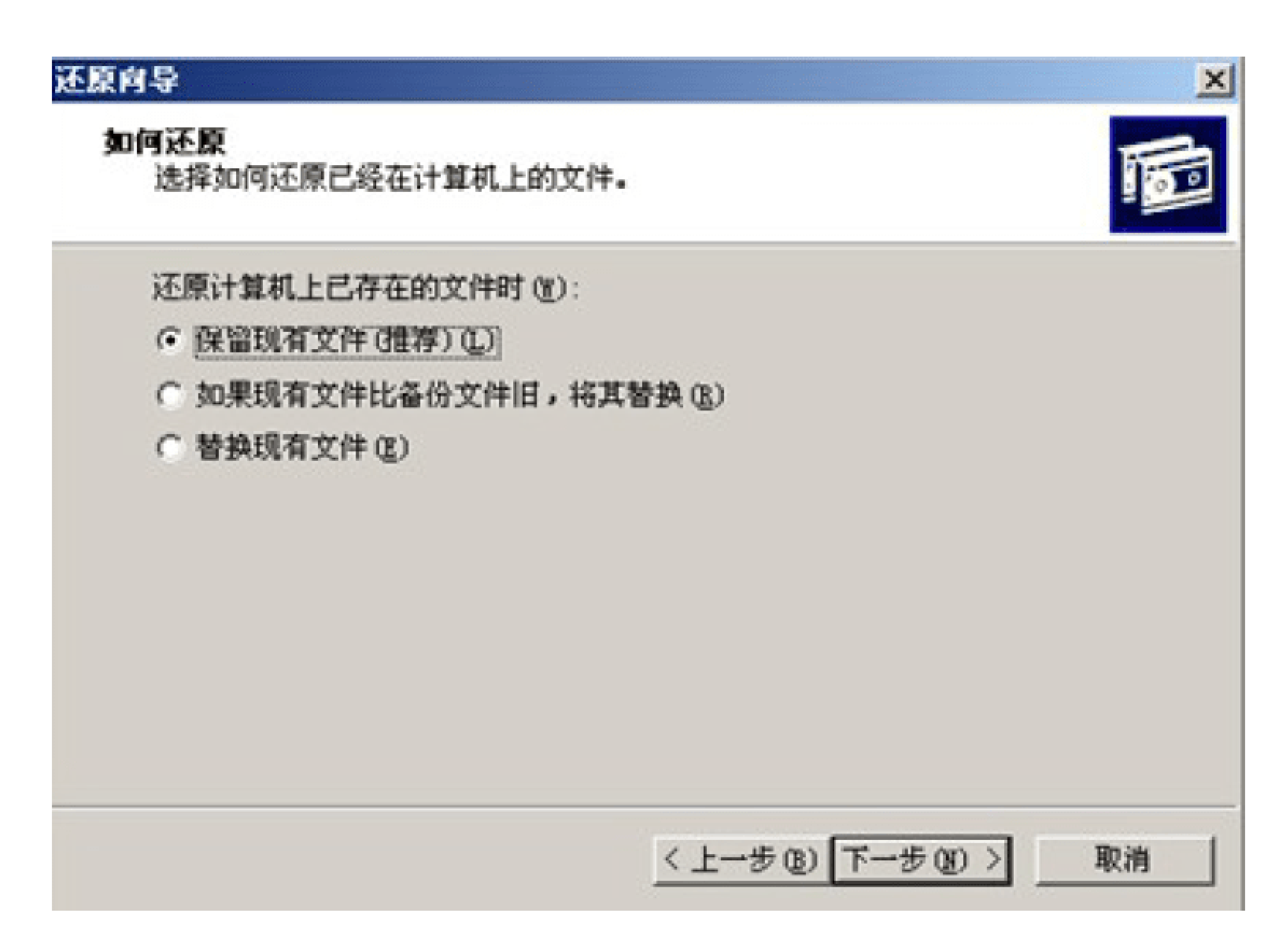


图 19-11　选择如何还原

图 19-12　开始还原

① 使用安全模式。

情景描述：公司服务器因为配置错误或驱动错误等原因无法正常启动，于是管理员决定使用安全模式启动计算机，以便更改系统配置来排除错误。

操作方法：启动时按 F8 键进入，如图 19-13 所示。

说明

安全模式只启动基本设备和驱动程序，操作系统使用系统默认设置；利用安全模式启动后，可以通过修改注册表、修改系统配置、重新安装驱动程序等来解决系统故障。

② 故障恢复控制台。

情景描述：管理员小张发现服务器使用安全模式也无法启动，这时可以通过故障恢复控制台来引导系统，尝试修正系统故障。

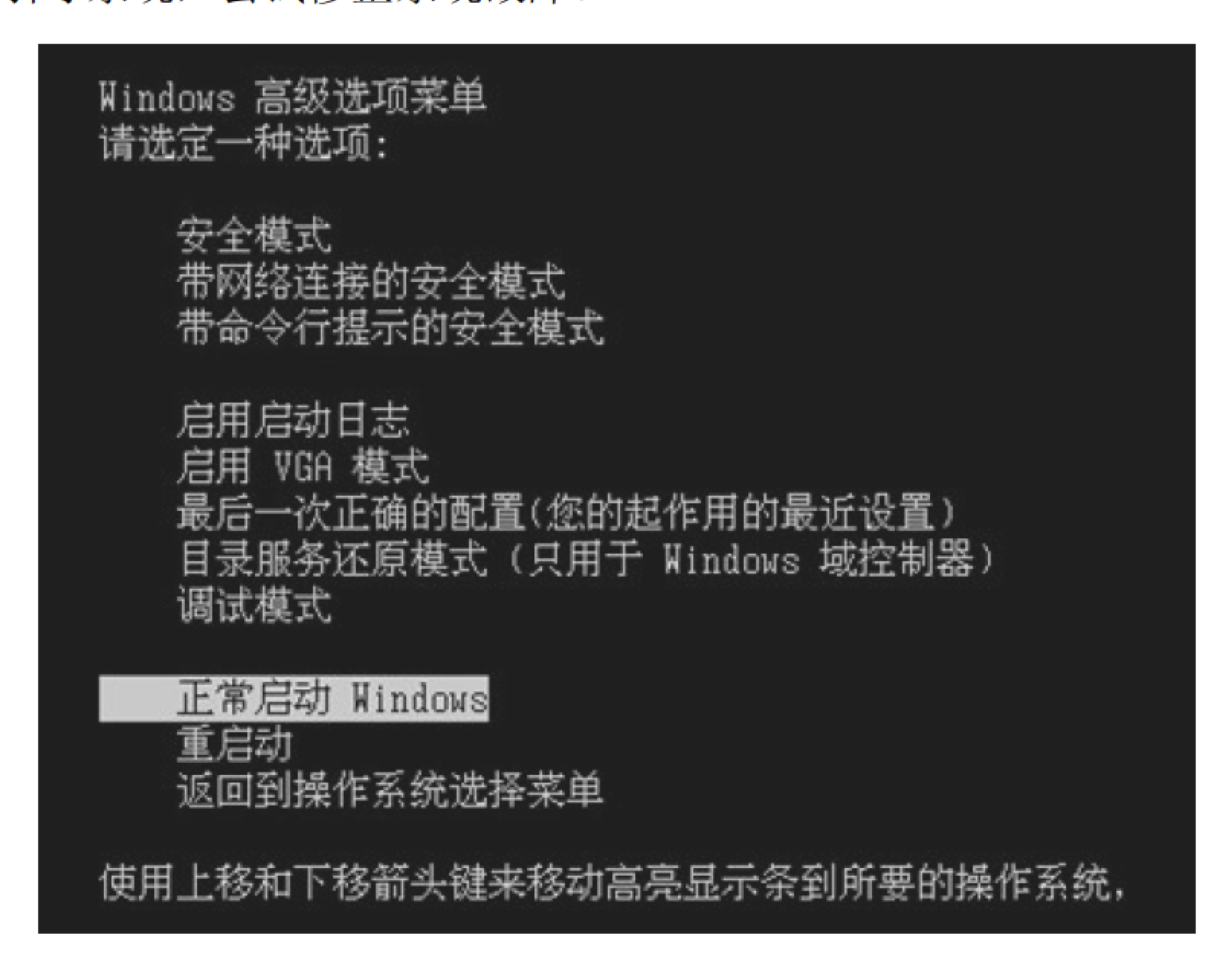


图 19-13　系统启动

操作方法：

方法1：插入安装光盘，使用光盘启动后选择故障恢复控制台模式，如图 19-14 所示。



图 19-14　选择恢复模式

方法 2：也可以事先在硬盘上安装故障恢复控制台。其安装方法：插入 Windows server 2003 安装光盘，然后运行光盘的 I386 文件夹中的 winnt32.exe 程序（“winnt32/cmdcons”）。

③使用“自动系统故障恢复准备向导”修复系统。当前两种方法都不能修复系统时，可以选择还原所有的启动卷和系统卷，这要求事先有所有卷的备份。一般重要的服务器都要求对整个系统进行备份，包括所有的启动卷和系统卷。但这种方法需要花费很多的时间。

管理员可以事先创建“自动恢复”软盘，并备份系统数据，当系统崩溃时，用它们来恢复系统。管理员可以使用 Windows Server 2003 的备份工具来创建“自动恢复”软盘和备份系统数据。

注：系统数据备份只能备份 Windows Server 2003 所在分区的数据。

下面是使用“自动系统故障恢复准备向导”备份系统数据的步骤。

①打开“备份”工具，选择“自动系统恢复向导”。②在“备份目的地”中，输入文件来存放系统数据。③单击“完成”按钮，开始复制系统数据。④最后按要求插入空白软盘，完成后给出如图 19-15 所示的提示对话框。（如果服务器没有软驱，可以将“%systemroot%\repair”目录中的 asr.sif 和 asrpnp.sif 文件复制到具有软驱的其他计算机上，然后将这些文件复制到软盘。）



图 19-15 “备份工具”提示框

使用备份数据恢复系统的步骤如下。

①使用 Windows Server2003 安装光盘启动系统，根据系统提示按 R 键选择“修复或者恢复”。②然后按 D 键，选择“自动系统恢复”。③根据系统提示操作。

实 例 小 结

没有任何一个系统是绝对安全可靠的，服务器随时可能因为硬件或软件的突发故障而导致灾难性的数据丢失。对关键数据的及时备份，是保证系统和数据安全的重要手段，是服务器管理工作中必不可少的一部分。Windows 操作系统为文件夹和文件提供“存档”属性，作为备份的依据。备份类型包括正常备份、副本备份、增量备份、差异备份、每日备份。需要根据要备份数据的内容制订合理的备份策略，如正常备份和差异备份相结合、正常备份和增量备份相结合等策略。备份操作通常使用系统的备份工具来完成，可以是手工备份或自动备份。发生数据丢失后，可以使用备份还原工具来进行数据还原。

如果因为管理员错误的配置、错误的驱动程序等原因造成服务器不能正常启动或正常使用时，可以用安全模式、系统还原、故障恢复控制台等方法来尝试修复系统。

附录 A

附表 A–1　维护常见安全漏洞列表的网站

组织名称	网站地址	描述
SANS	http://www.sans.org/top20	排在 SANS/FBI 前 20 的漏洞列表
SecurityFocus	http://www.seturityfocus.com/bid	软件漏洞事实上的标准
CommonVulnerabilities andExposure	http://www.cev.mitre.org	系统漏洞及其他安全隐患的标准化名称列表
CERT Coordination Certer	http://www.cert.org/nav/index-red.html	CERT 漏洞，事故以及补丁
Securia	http://securia.com	漏洞列表及安全报告

附表 A–2　安全扫描工具的网站

组织名称	网站地址	产品名称	成本
Nessus	http://www.nessus.org	Nessus 安全扫描工具	免费
微软公司	http://www.microsoft.com/technet/security/tools/mbsahome.mspx	微软 Baseline 安全分析器	免费
Foundstone	http://www.foundstone.com	Foundstone Professional	每年 12000 美元
Insecure.org	http://www.insecure.org	Nmap	免费
GFi	http://www.gif.com	GFi LanGuard	499 美元
Internet 安全中心	http://www.cisecurity.org	CIS 安全基准及得分工具	免费

附表 A–3　操作系统指纹识别工具

组织名称	网站地址	产品名称
Insecure.org	http://www.insecure.org	Nmap
Safemode.org	http://www.safemode.org/sprint/	Sprint
Sys-Security Group	http://www.sys-security.com/html/projects/X.html	Xprobe2

附表 A–4　安全漏洞邮寄列表

组织名称	网站地址	描述
Security Focus	http://www.securityfocus.com/subscribe?listname=1	最新的漏洞邮寄名单
SANS Institute	http://www.sans.org/newsletters/	SANS 通信及邮寄列表摘要订阅
Sintelli	http://www.sintelli.com	SINTRAQ 安全漏洞邮寄列表

附录 A–5　黑 客 大 会

1．BlackHat

http://www.blackhat.com/

2．CanSecWest

http://www.cansecwest.com/

3．defcon

http://www.defcon.org

4．Hacker&Phreaker

5．HackerZ Hideout

6．Hacker's　haven

部分信息安全相关网址：

http://www.cs.tufts.edu/~mcable/cypher/alerts/alerts.html (Cypherpunk)
http://www.cs.tufts.edu/~mcable/HackerCrackdown (Hacker Crackdown)
http://www.cs.umd.edu/~lgas
http://www.cs.cmu.edu:8001/afs/cs.cmu.edu/user/bsy/www/sec.html (Security)
http://www.csd.harris.com/secure_info.html (Harris)
http://www.csl.sri.com/ (SRI Computer Science Lab)
http://www.cybercafe.org/cybercafe/pubtel/pubdir.html (CyberCafe)
http://www.datafellows.fi/ (Data Fellows)
http://www.delmarva.com/raptor/raptor.html (Raptor Network Isolator)
http://www.demon.co.uk/kbridge (KarlBridge)
http://www.digicash.com/ecash/ecash-home.html (Digital Cash)
http://www.digital.com/info/key-secure-index.html(Digital Secure Systems)
http://www.eecs.nwu.edu/~jmyers/bugtraq/index.html(Bugtraq)
http://www.eecs.nwu.edu/~jmyers/ids/index.html (Intrusion Detection Systems)
http://www.eff.org/papers.html (EFF)
http://www.engin.umich.edu/~jgotts/boxes.html (Box info)
http://www.engin.umich.edu/~jgotts/hack-faq.html(This document)
http://www.engin.umich.edu/~jgotts/underground.html
http://www.ensta.fr/internet/unix/sys_admin (System administration)
http://www.etext.org/Zines/ (Zines)
http://www.fc.net/defcon (DefCon)

http://www.fc.net/phrack.html (Phrack Magazine)
http://www.first.org/first/ (FIRST)
http://www.greatcircle.com/ (Great Circle Associates)
http://www.ic.gov/ (The CIA)
http://www.lerc.nasa.gov/Unix_Team/Dist_Computing_Security.html (Security)
http://www.lysator.liu.se:7500/terror/thb_title.html (Terrorists Handbook)
http://www.lysator.liu.se:7500/mit-guide/mit-guide.html (Lockpicking Guide)
http://www.net23.com/ (Max Headroom)
http://www.nist.gov/ (NIST)
http://www.pacbell.com/ (Pacific Bell)
http://www.paranoia.com/mthreat (ToneLoc)
http://www.pegasus.esprit.ec.org/people/arne/pgp.html (PGP)
http://www.phantom.com/~king (Taran King)
http://www.quadralay.com/www/Crypt/Crypt.html (Quadralay Cryptography)
http://www.qualcomm.com/cdma/wireless.html (Qualcomm CDMA)
http://www.research.att.com/ (AT&T)
http://ripco.com:8080/~glr/glr.html (Full Disclosure)
http://www.rsa.com/ (RSA Data Security)
http://www.satelnet.org/~ccappuc
http://www.service.com/cm/uswest/usw1.html (USWest)
http://www.shore.net/~oz/welcome.html (Hack TV)
http://www.spy.org/ (Computer Systems Consulting)
http://www.sri.com/ (SRI)
http://www.tansu.com.au/Info/security.html (Security Reference Index)
http://www.tis.com/ (Trusted Information Systems)
http://www.tri.sbc.com/ (Southwestern Bell)
http://www.uci.agh.edu.pl/pub/security (Security)
http://www.umcc.umich.edu/~doug/virus-faq.html (Virus)
http://www.usfca.edu/crackdown/crack.html (Hacker Crackdown)
http://www.wam.umd.edu/~ankh/Public/devil_does_unix
http://www.wiltel.com/ (Wiltel)
http://www.winternet.com/~carolann/dreams.html
http://www.wired.com/ (Wired Magazine)
http://www.hacker.org/undertop.html
http://www.ilf.net/

参 考 文 献

[1] 刘克龙，冯登国，石文昌．安全操作系统原理和技术[M]．北京：科学出版社，2004．

[2] 卢开澄．计算机密码学：计算机网络的数据保密与安全[M]．2 版．北京：清华大学出版社，1998．

[3] 宁蔡．访问控制安全技术及应用[M]．北京：电子工业出版社，2005．

[4] 卿斯汉．安全协议[M]．北京：清华大学出版社，2005．

[5] 沈昌祥．信息安全工程导论[M]．北京：电子工业出版社，2003．

[6] 施伯乐，丁宝康，汪卫．数据库系统教程[M]．2 版．北京：高等教育出版社，2003．

[7] 邵祖英，王英彬．计算机局部网络[M]．北京：清华大学出版社，1989．

[8] 唐正军，李建华．入侵检测技术[M]．北京：清华大学出版社，2004．

[9] 汤子瀛，哲凤屏，汤小丹．计算机操作系统[M] ．西安：西安电子科技大学出版社，1996．

[10] Bauer FL，吴世忠．密码编码和密码分析原理与方法[M]．宋晓龙，李守鹏，译．北京：机械工业出版社，2001．

[11] 许国安，顾基发，车宏安．系统科学[M]．上海：上海科技教育出版社，2000．

[12] 晓宗．信息安全信息站[M]．北京：清华大学出版社，2004．

[13] 严蔚敏．数据结构[M]．北京：清华大学出版社，1997．

[14] 张敏，徐震，冯登国．数据库安全[M]．北京：科学出版社，2005．

[16] 赵战生，杜虹，吕述望．信息安全保密教程[M]．北京：中国科学技术大学出版社，北京：北京中电电子出版社，2006．

[17] 张玉清，戴祖峰，谢崇斌．安全扫描技术[M]．北京：清华大学出版社，2004．

[18] 谢希仁．计算机网络[M]．北京：电子工业出版社，2008．

[19] Michael Howard，David LeBlanc．编写安全的代码[M]．微软出版社，2003．